Fixlet ID	Name
363	Block Automatic Delivery of IE 7 - Windows XP SP2/Windows Server 2003 SP1
364	Unblock Automatic Delivery of IE 7 - Windows XP SP2/Windows Server 2003 SP1
372	Block Automatic Delivery of IE 7 - Windows XP/2003 (x64)
373	Unblock Automatic Delivery of IE 7 - Windows XP/2003 (x64)
390	UPDATE: Microsoft .NET Framework 3.5 Available - Windows XP/2003/Vista
391	UPDATE: Microsoft .NET Framework 3.5 Available - Windows XP/2003/Vista (x64)
392	UPDATE: Microsoft .NET Framework 2.0 SP1 Available - Windows 2000
394	UPDATE: Microsoft .NET Framework 2.0 SP1 Available - Windows 2000 (Security Update Needed)
396	UPDATE: Microsoft .NET Framework 2.0 SP1 Available - Windows XP/2003
397	UPDATE: Microsoft .NET Framework 2.0 SP1 Available - Windows XP/2003 (x64)
399	Block Delivery of Windows XP Service Pack 3
401	Unblock Delivery of Windows XP Service Pack 3
402	Block Delivery of Windows Vista Service Pack 1
403	Unblock Delivery of Windows Vista Service Pack 1
440	Block Delivery of Windows Vista Service Pack 1 (x64)
441	Unblock Delivery of Windows Vista Service Pack 1 (x64)
443	Office XP Sample Fixlet - Internal Use Only
448	UPDATE: Microsoft .NET Framework 3.5 SP1 Available - Windows XP/2003/Vista/2008
458	Block Automatic Delivery of IE 8 - Windows XP/2003/Vista/2008
459	Unblock Automatic Delivery of IE 8 - Windows XP/2003/Vista/2008
460	Block Automatic Delivery of IE 8 - Windows XP/2003/Vista/2008 (x64)
461	Unblock Automatic Delivery of IE 8 - Windows XP/2003/Vista/2008 (x64)
486	UPDATE: Windows Vista Service Pack 2 Available (x64) - Known Issues
488	UPDATE: Windows Vista Service Pack 2 Available (x64)
570	Block Automatic Delivery of IE 9 - Windows Vista/2008/7/2008 R2 (x64)
574	Unblock Automatic Delivery of IE 9 - Windows Vista/2008/7/2008 R2 (x64)
575	Unblock Automatic Delivery of IE 9 - Windows Vista/2008/7
576	Block Automatic Delivery of IE 9 - Windows Vista/2008/7
578	Block Automatic Delivery of IE 10 - Windows 7 SP1
580	Block Automatic Delivery of IE 10 - Windows 7 SP1/2008 R2 SP1 (x64)
581	Unblock Automatic Delivery of IE 10 - Windows 7 SP1
582	Unblock Automatic Delivery of IE 10 - Windows 7 SP1/2008 R2 SP1 (x64)
583	Block Automatic Delivery of IE 11 - Windows 7 SP1

585	Block Automatic Delivery of IE 11 - Windows 7 SP1/2008 R2 SP1 (x64)
587	Unblock Automatic Delivery of IE 11 - Windows 7 SP1
589	Unblock Automatic Delivery of IE 11 - Windows 7 SP1/2008 R2 SP1 (x64)
701	Microsoft Warning: Windows 7 SP1 going out of support
11301	UPDATE: Windows NT Security Rollup Package
11303	UPDATE: Windows NT Terminal Server Edition Post-Sp6 Security Rollup Package Available
12201	UPDATE: Windows 2000 Service Pack 2 Available
12202	UPDATE: Windows 2000 Service Pack 3 Available
12301	UPDATE: Windows 2000 Security Rollup Package 1
13406	(Mechanism to Disable Delivery of Windows XP SP2 Expires on April 12th
13502	UPDATE: Windows XP Service Pack 3 Available - Known Issues - Free Space
13503	UPDATE: Windows XP Service Pack 3 Available - Known Issues - RDP 6.0 MUI Pack
14101	UPDATE: Windows Media Player 7.1 Available
15110	UPDATE: MDAC 2.8 Service Pack 1 Available
20337	UPDATE: SQL Server 2005 Express Service Pack 3 Available
20343	UPDATE: SQL Server 2005 Express Service Pack 4 Available
23113	UPDATE: Internet Explorer 7 Available - Windows XP SP2/SP3 (BES Console Installed) (Superseded)
23114	UPDATE: Internet Explorer 7 Available - Windows Server 2003 SP1/SP2 (BES Console Installed) (Superseded)
23116	UPDATE: Internet Explorer 7 Available - IE 7 Beta Installed - Windows XP/2003
23117	UPDATE: Internet Explorer 7 Available - IE 7 Beta Installed - Windows XP/2003 (x64)
23119	UPDATE: Internet Explorer 7 Available - Windows XP/2003 (x64) (BES Console Installed) (Superseded)
23120	UPDATE: Internet Explorer 7 Available - Windows Server 2003 SP1/SP2 (Superseded)
23122	UPDATE: Internet Explorer 7 Available - Windows XP SP2/SP3 (Superseded)
23124	UPDATE: Internet Explorer 7 Available - Windows XP/2003 (x64) (Superseded)
23131	UPDATE: Internet Explorer 8 Available - Windows XP SP2/SP3
23132	UPDATE: Internet Explorer 8 Available - Windows XP SP2/SP3 - CORRUPT PATCH
23133	UPDATE: Internet Explorer 8 Available - Windows Server 2003 SP2
23134	UPDATE: Internet Explorer 8 Available - Windows Server 2003 SP2 - CORRUPT PATCH

23135	UPDATE: Internet Explorer 8 Available - Windows Vista Gold - Prerequisites Required
23136	UPDATE: Internet Explorer 8 Available - Windows Vista/2008 (Superseded)
23137	UPDATE: Internet Explorer 8 Available - Windows XP/2003 (x64)
23138	UPDATE: Internet Explorer 8 Available - Windows XP/2003 (x64) - CORRUPT PATCH
23139	UPDATE: Internet Explorer 8 Available - Windows Vista Gold - Prerequisites Required (x64)
23140	UPDATE: Internet Explorer 8 Available - Windows Vista/2008 (x64) (Superseded)
23150	UPDATE: Internet Explorer 9 Available - Prerequisites - Windows Vista SP2 / Windows Server 2008 SP2
23151	UPDATE: Internet Explorer 9 Available - Install - Windows Vista SP2 / Windows Server 2008 SP2 (Superseded)
23152	UPDATE: Internet Explorer 9 Available - Prerequisites - Windows 7 (Superseded)
23154	UPDATE: Internet Explorer 9 Available - Prerequisites - Windows Vista SP2 / Windows Server 2008 SP2 (x64)
23155	UPDATE: Internet Explorer 9 Available - Install - Windows Vista SP2 / Windows Server 2008 SP2 (x64) (Superseded)
23156	UPDATE: Internet Explorer 9 Available - Prerequisites - Windows 7 / Windows Server 2008 R2 (x64)
24202	UPDATE: Microsoft .NET Framework 1.0 Service Pack 2 Available
24203	UPDATE: Microsoft .NET Framework 1.0 Service Pack 3 Available
25201	UPDATE: Windows Installer 3.0 for Windows 2000/XP/2003
25202	UPDATE: Windows Installer 3.1 for Windows 2000/XP/2003
25205	UPDATE: Windows Installer 3.1 update for Windows XP (x64)
25208	UPDATE: Windows Installer 3.1 update for Windows XP (x64) - CORRUPT PATCH
25215	UPDATE: Windows Installer 4.5 for Windows XP SP2/SP3
25216	UPDATE: Windows Installer 4.5 for Windows XP SP2/SP3 - CORRUPT PATCH
25217	UPDATE: Windows Installer 4.5 for Windows XP (x64)
25218	UPDATE: Windows Installer 4.5 for Windows XP (x64) - CORRUPT PATCH
28206	UPDATE: Office 2000 SP-3 Update Available - Windows NT/2000/XP (Administrative Installation)
28302	UPDATE: Office 2000 SP-3 Update Available - MultiLanguage Pack Disc 1 - Windows NT/2000/XP/2003 (Network Installation)
28304	UPDATE: Office 2000 SP-3 Update Available - MultiLanguage Pack Disc 2 - Windows NT/2000/XP/2003 (Network Installation)
28306	UPDATE: Office 2000 SP-3 Update Available - MultiLanguage Pack Disc 3 - Windows NT/2000/XP/2003 (Network Installation)

28308	UPDATE: Office 2000 SP-3 Update Available - MultiLanguage Pack Disc 4 - Windows NT/2000/XP/2003 (Network Installation)
28310	UPDATE: Office 2000 SP-3 Update Available - MultiLanguage Pack Disc 5 - Windows NT/2000/XP/2003 (Network Installation)
28312	UPDATE: Office 2000 SP-3 Update Available - MultiLanguage Pack Disc 6 - Windows NT/2000/XP/2003 (Network Installation)
28314	UPDATE: Office 2000 SP-3 Update Available - MultiLanguage Pack Disc 7 - Windows NT/2000/XP/2003 (Network Installation)
28316	UPDATE: Office 2000 SP-3 Update Available - MultiLanguage Pack Disc 8 - Windows NT/2000/XP/2003 (Network Installation)
28320	UPDATE: Office 2000 SP-3 Update Available - MultiLanguage Packs - Windows NT/2000/XP/2003 (Administrative Installation)
28401	UPDATE: Office 2000 Service Release 1 (SR-1a) Update - Windows NT/2000/XP (Administrative Installation)
29201	UPDATE: Office XP Service Pack 1 Available - Windows NT/2000/XP (Administrative Installation)
29202	UPDATE: Office XP Service Pack 1 Available - Windows NT/2000/XP (Network Installation)
29203	UPDATE: Office XP Service Pack 1 Available - (Local Installation)
29204	UPDATE: Office XP Service Pack 1 Available - Windows 9x/ME (Administrative Installation)
29205	UPDATE: Office XP Service Pack 1 Available - Windows 9x/ME (Network Installation)
29206	UPDATE: Office XP Service Pack 2 Available - Windows NT/2000/XP (Administrative Installation)
29209	UPDATE: Office XP Service Pack 2 Available - Windows 9x/ME (Administrative Installation)
29211	UPDATE: Office XP Service Pack 3 Available - Windows NT/2000/XP (Administrative Installation)
29214	UPDATE: Office XP Service Pack 3 Available - Windows 9x/ME (Administrative Installation)
29227	UPDATE: Office XP Service Pack 3 MUI Available - Windows NT/2000/XP/2003 (Administrative Installation)
29229	UPDATE: Office XP Service Pack 3 MUI Available - Windows 9x/ME (Administrative Installation)
38101	UPDATE: Office 2003 Service Pack 1 Available - Windows 2000/XP/2003 (Administrative Installation)
38102	UPDATE: Office 2003 Service Pack 1 Available - Windows 2000/XP/2003 (Local Installation)
38103	UPDATE: Office 2003 Service Pack 1 Available (Web Components 10) - Windows 2000/XP/2003 (Network/Local Installation)
38104	UPDATE: Office 2003 Service Pack 1 Available (Web Components 11) - Windows 2000/XP/2003 (Network/Local Installation)

38105	UPDATE: Office 2003 Service Pack 1 Available - Windows 2000/XP/2003 (Network Installation)
38106	UPDATE: Office 2003 Service Pack 2 Available - Windows 2000/XP/2003 (Local Installation)
38107	UPDATE: Office 2003 Service Pack 2 Available - Windows 2000/XP/2003 (Administrative Installation)
38108	UPDATE: Office 2003 Service Pack 2 Available - Windows 2000/XP/2003 (Network Installation)
38110	UPDATE: Office 2003 Service Pack 2 Available (Web Components 10) - Windows 2000/XP/2003
38111	UPDATE: Office 2003 Service Pack 2 Available (Web Components 11) - Windows 2000/XP/2003
38112	UPDATE: Office 2003 Service Pack 2 for MUI Available - Windows 2000/XP/2003 (Network/Local Installation)
38115	UPDATE: Office 2003 Service Pack 2 for MUI Available - Windows 2000/XP/2003 (Administrative Installation)
38121	UPDATE: Office 2003 Service Pack 3 for MUI Available - Windows 2000/XP/2003/Vista (Network/Local Installation)
38122	UPDATE: Office 2003 Service Pack 3 for MUI Available - Windows 2000/XP/2003/Vista (Administrative Installation)
38201	UPDATE: Office 2003 Service Pack 2 for Proofing Tools Available - Windows 2000/XP/2003 (Local Installation)
38202	UPDATE: Office 2003 Service Pack 2 for Proofing Tools Available - Windows 2000/XP/2003 (Network Installation)
38203	UPDATE: Office 2003 Service Pack 2 for Proofing Tools Available - Windows 2000/XP/2003 (Administrative Installation)
38204	UPDATE: Office 2003 Service Pack 3 for Proofing Tools Available - Windows 2000/XP/2003/Vista (Local Installation)
38205	UPDATE: Office 2003 Service Pack 3 for Proofing Tools Available - Windows 2000/XP/2003/Vista (Network Installation)
38206	UPDATE: Office 2003 Service Pack 3 for Proofing Tools Available - Windows 2000/XP/2003/Vista (Administrative Installation)
40101	UPDATE: Microsoft .NET Framework 1.1 Service Pack 1 Available - Windows 98/ME/NT/2000/XP
40107	UPDATE: Microsoft .NET Framework 1.1 Service Pack 1 Available - Windows 2008 / Windows Vista
40201	UPDATE: Microsoft .NET Framework 1.1 Available - Windows 2000/XP/2003/Vista/2008
40301	UPDATE: Microsoft .NET Framework 4.0 Available
40401	UPDATE: Microsoft .NET Framework 4.0 Client Profile Available
41101	UPDATE: Microsoft Proxy Server 2.0 Service Pack 1 Available - Windows NT Server

41102	UPDATE: Microsoft Proxy Server 2.0 Service Pack 1 Available - Windows NT Server - CORRUPT PATCH
44601	UPDATE: Windows Vista Service Pack 1 Available
44602	UPDATE: Windows Vista Service Pack 1 Available (x64)
44603	UPDATE: Windows Vista Service Pack 1 Available - Known Issues
44604	UPDATE: Windows Vista Service Pack 1 Available (x64) - Known Issues
44605	UPDATE: Windows Vista Service Pack 1 Available - Installation Not Complete
44606	UPDATE: Windows Vista Service Pack 1 Available (x64) - Installation Not Complete
44701	UPDATE: Windows Vista Service Pack 2 Available
44703	UPDATE: Windows Vista Service Pack 2 Available - Known Issues
44705	UPDATE: Windows Vista Service Pack 2 Available - Installation Not Complete
44706	UPDATE: Windows Vista Service Pack 2 Available (x64) - Installation Not Complete
45001	UPDATE: Microsoft .NET Framework 4.5 Available - Windows 7 SP1 / Windows 2008 SP2 / Windows 2008 R2 SP1 / Windows Vista SP2
45101	UPDATE: Microsoft .NET Framework 4.5.1 Available - Windows Vista SP2 / Windows 7 SP1 / Windows 8 / Windows Server 2008 SP2 / Windows Server 2008 R2 SP1 / Windows Server 2012
45204	UPDATE: Windows Server 2003 Service Pack 2 Available - Windows XP/2003 (x64)
45205	UPDATE: Windows Server 2003 Service Pack 2 Available - Known Issues - Free Space - Windows XP/2003 (x64)
45206	UPDATE: Windows Server 2003 Service Pack 2 Available - Pending Restart - Windows XP/2003 (x64)
45207	UPDATE: Windows Server 2003 Service Pack 2 Available - Known Issues - MSDTC - Windows XP/2003 (x64)
46103	UPDATE: Visio 2003 Service Pack 2 - Windows 2000/XP/2003 (Network/Local Installation)
46104	UPDATE: Visio 2003 Service Pack 2 for MUI Korean - Windows 2000/XP/2003 (Network/Local Installation)
47101	UPDATE: Project 2003 Service Pack 2 - Windows 2000/XP/2003 (Network/Local Installation)
47102	UPDATE: Project 2003 Service Pack 2 for Korean MUI - Windows 2000/XP/2003 (Network/Local Installation)
48001	UPDATE: Microsoft .NET Framework 4.8 Available - Windows 7 SP1 / Windows 8.1 / Windows 2008 R2 SP1 / Windows 2012 / Windows 2012 R2 / Windows 10 / Windows Server 2016 / Windows Server 2019
48101	UPDATE: OneNote 2003 Service Pack 2 - Windows 2000/XP/2003 (Network/Local Installation)
52104	UPDATE: Visual Web Dev Express Edition Service Pack 1

52107	UPDATE: Visual C# Express Edition Service Pack 1
52108	UPDATE: Visual J# Express Edition Service Pack 1
55201	UPDATE: Microsoft .NET Framework 3.5 SP1 Update Available - Windows XP/2003
55202	UPDATE: Microsoft .NET Framework 3.5 SP1 Update Available - Windows Vista/2008
55203	UPDATE: Microsoft .NET Framework 3.5 SP1 Update Available - Windows XP/2003 (x64)
55204	UPDATE: Microsoft .NET Framework 3.5 SP1 Update Available - Windows Vista/2008 (x64)
57001	UPDATE: Microsoft .NET Framework 2.0 SP2 Available - Windows XP/2003
57002	UPDATE: Microsoft .NET Framework 2.0 SP2 Available - Windows XP/2003 (x64)
57003	UPDATE: Microsoft .NET Framework 2.0 SP2 Available - Windows XP/2003 - CORRUPT PATCH
57004	UPDATE: Microsoft .NET Framework 2.0 SP2 Available - Windows XP/2003 (x64) - CORRUPT PATCH
67001	UPDATE: Windows 7 Service Pack 1 Available
67003	UPDATE: Windows 7 Service Pack 1 Available - Known Issues
67005	UPDATE: Windows 7 Service Pack 1 Available - Installation Not Complete
70001	UPDATE: Windows 7 Service Pack 1 Available (x64)
70003	UPDATE: Windows 7 Service Pack 1 Available (x64) - Known Issues
70005	UPDATE: Windows 7 Service Pack 1 Available (x64) - Installation Not Complete
100102	MS01-001: Web Client Authentication Vulnerability in Windows ME
100103	MS01-001: Web Client Authentication Vulnerability in Windows ME - CORRUPT PATCH
101701	MS01-017: Erroneous VeriSign Certificate Vulnerability
101702	MS01-017: Erroneous VeriSign Certificate Vulnerability - CORRUPT PATCH
102201	MS01-022: "WebDAV Service Provider" Vulnerability
103901	MS01-039: Services for Unix 2.0 NFS Vulnerability - Windows 2000
103902	MS01-039: Services for Unix 2.0 NFS Vulnerability - Windows 2000 - CORRUPT PATCH
103903	MS01-039: Services For Unix 2.0 NFS Vulnerability - Windows NT
103904	MS01-039: Services For Unix 2.0 NFS Vulnerability - Windows NT - CORRUPT PATCH
103905	MS01-039: Services for Unix 2.0 Telnet Vulnerability - Windows 2000
103906	MS01-039: Services for Unix 2.0 Telnet Vulnerability - Windows 2000 - CORRUPT PATCH
103907	MS01-039: Services for Unix 2.0 Telnet Vulnerability - Windows NT

104301	MS01-043: NNTP Service in Windows NT 4.0 Contains Memory Leak
104302	MS01-043: NNTP Service in Windows NT 4.0 Contains Memory Leak - CORRUPT PATCH
105002	MS01-050: "Malformed Document" Vulnerability in PowerPoint 2000 - Windows NT/2000/XP (Administrative Installation)
105004	MS01-050: "Malformed Document" Vulnerability in PowerPoint 2000 - Windows NT/2000/XP (Network Installation)
105203	MS01-052: "Invalid RDP Data" Vulnerability in Windows 2000 Server/Advanced Server
105204	MS01-052: "Invalid RDP Data" Vulnerability in Windows 2000 Server/Advanced Server - CORRUPT PATCH
105603	MS01-056: "Unchecked Buffer" in Windows Media Player .ASF Processor - Windows XP
105604	MS01-056: "Unchecked Buffer" in Windows Media Player .ASF Processor - Windows XP - CORRUPT PATCH
105901	MS01-059: Unchecked Universal Plug and Play Buffer in WinXP
105902	MS01-059: Unchecked Universal Plug and Play Buffer in WinXP - CORRUPT PATCH
105903	MS01-059: Unchecked Universal Plug and Play Buffer in WinME
105904	MS01-059: Unchecked Universal Plug and Play Buffer in WinME - CORRUPT PATCH
105905	MS01-059: Unchecked Universal Plug and Play Buffer in Win98
105906	MS01-059: Unchecked Universal Plug and Play Buffer in Win98 - CORRUPT PATCH!Win98!Thu, 20 Dec 200
200101	MS02-001: Trusting Domains Do Not Verify Domain Membership of SIDs in Authorization Data
200601	MS02-006: SNMP Service Unchecked Buffer in Windows 2000
200602	MS02-006: SNMP Service Unchecked Buffer in Windows 2000 - CORRUPT PATCH
200603	MS02-006: SNMP Service Unchecked Buffer in Windows XP
200604	MS02-006: SNMP Service Unchecked Buffer in Windows XP - CORRUPT PATCH
200605	MS02-006: SNMP Service Unchecked Buffer in Windows NT
200606	MS02-006: SNMP Service Unchecked Buffer in Windows NT - CORRUPT PATCH
200607	MS02-006: SNMP Service Unchecked Buffer in Windows NT, TSE
200608	MS02-006: SNMP Service Unchecked Buffer in Windows NT, TSE - CORRUPT PATCH
200609	MS02-006: SNMP Service Unchecked Buffer in Windows 98
200610	MS02-006: SNMP Service Unchecked Buffer in Windows 98 - CORRUPT PATCH
200611	MS02-006: SNMP Service Unchecked Buffer in Windows 95

201104	MS02-011: Authentication Flaw in SMTP Service - Windows NT Server - CORRUPT PATCH
201201	MS02-011,012: Windows 2000 SMTP Patch
201202	MS02-011,012: Windows 2000 SMTP Patch - CORRUPT PATCH
201203	MS02-012: Windows XP SMTP Patch
201204	MS02-012: Windows XP SMTP Patch - CORRUPT PATCH
201401	MS02-014: Unchecked Buffer in Windows 98 Shell Could Lead to Code Execution
201402	MS02-014: Unchecked Buffer in Windows 98 Shell Could Lead to Code Execution - CORRUPT PATCH
201601	MS02-016: Opening Group Policy Files for Exclusive Read Blocks Policy Application
201701	MS02-017: Unchecked buffer in the Multiple UNC Provider - Windows NT
201702	MS02-017: Unchecked buffer in the Multiple UNC Provider - Windows NT - CORRUPT PATCH
201703	MS02-017: Unchecked buffer in the Multiple UNC Provider - Windows NT Terminal Server
201704	MS02-017: Unchecked buffer in the Multiple UNC Provider - Windows NT Terminal Server - CORRUPT PATCH
201705	MS02-017: Unchecked buffer in the Multiple UNC Provider - Windows 2000
201706	MS02-017: Unchecked buffer in the Multiple UNC Provider - Windows 2000 - CORRUPT PATCH
201707	MS02-017: Unchecked buffer in the Multiple UNC Provider - Windows XP
201708	MS02-017: Unchecked buffer in the Multiple UNC Provider - Windows XP - CORRUPT PATCH
202401	MS02-024: Windows NT Debugger Authentication Flaw
202402	MS02-024: Windows NT Debugger Authentication Flaw - CORRUPT PATCH
202403	MS02-024: Windows NT Terminal Server Debugger Authentication Flaw
202404	MS02-024: Windows NT Terminal Server Debugger Authentication Flaw - CORRUPT PATCH
202405	MS02-024: Windows 2000 Debugger Authentication Flaw
202406	MS02-024: Windows 2000 Debugger Authentication Flaw - CORRUPT PATCH
202703	MS02-027: Unchecked Buffer in Gopher Protocol Handler for Proxy Server 2.0
202801	MS02-028: Heap Overrun in HTR chunked encoding - IIS 5.0
202803	MS02-028: Heap Overrun in HTR chunked encoding - IIS 4.0
202804	MS02-028: Heap Overrun in HTR chunked encoding - IIS 4.0 - CORRUPT PATCH
202901	MS02-029: Unchecked Buffer in RAS Phonebook for Windows NT 4.0

202902	MS02-029: Unchecked Buffer in RAS Phonebook for Windows NT 4.0 - CORRUPT PATCH
202903	MS02-029: Unchecked Buffer in RAS Phonebook for Windows XP
202904	MS02-029: Unchecked Buffer in RAS Phonebook for Windows XP - CORRUPT PATCH
202905	MS02-029: Unchecked Buffer in RAS Phonebook for Windows 2000
202906	MS02-029: Unchecked Buffer in RAS Phonebook for Windows 2000 - CORRUPT PATCH
202911	MS02-029: Unchecked Buffer in RAS Phonebook for Windows NT Terminal Server
202912	MS02-029: Unchecked Buffer in RAS Phonebook for Windows NT Terminal Server - CORRUPT PATCH
203201	MS02-032: 26 June 2002 Cumulative Patch for Windows Media Player 6.4
203203	MS02-032: 26 June 2002 Cumulative Patch for Windows Media Player 7.1
203701	MS02-037: Server Response To SMTP Client EHLO Command Results In Buffer Overrun
204501	MS02-045: Unchecked Buffer in Network Share Provider - Windows NT
204502	MS02-045: Unchecked Buffer in Network Share Provider - Windows NT - CORRUPT PATCH
204503	MS02-045: Unchecked Buffer in Network Share Provider - Windows XP
204504	MS02-045: Unchecked Buffer in Network Share Provider - Windows XP - CORRUPT PATCH
204505	MS02-045: Unchecked Buffer in Network Share Provider - Windows NT TSE
204506	MS02-045: Unchecked Buffer in Network Share Provider - Windows NT TSE - CORRUPT PATCH
204507	MS02-045: Unchecked Buffer in Network Share Provider - Windows 2000
204508	MS02-045: Unchecked Buffer in Network Share Provider - Windows 2000 - CORRUPT PATCH
204801	MS02-048: Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates - Windows XP
204802	MS02-048: Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates - Windows XP - CORRUPT PATCH
204803	MS02-048: Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates - Windows 2000
204804	MS02-048: Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates - Windows 2000 - CORRUPT PATCH
204805	MS02-048: Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates - Windows NT TSE

204806	MS02-048: Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates - Windows NT TSE - CORRUPT PATCH
204809	MS02-048: Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates - Windows ME
204811	MS02-048: Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates - Windows 98
205005	MS02-050: Certificate Validation Flaw Could Enable Identity Spoofing in Windows XP
205006	MS02-050: Certificate Validation Flaw Could Enable Identity Spoofing in Windows XP - CORRUPT PATCH
205007	MS02-050: Certificate Validation Flaw Could Enable Identity Spoofing in Windows 98
205008	MS02-050: Certificate Validation Flaw Could Enable Identity Spoofing in Windows ME
205009	MS02-050: Certificate Validation Flaw Could Enable Identity Spoofing in Windows 2000
205010	MS02-050: Certificate Validation Flaw Could Enable Identity Spoofing in Windows 2000 - CORRUPT PATCH
205103	MS02-051: Cryptographic Flaw in RDP Protocol can Lead to Information Disclosure - Windows XP
205104	MS02-051: Cryptographic Flaw in RDP Protocol can Lead to Information Disclosure - Windows XP - CORRUPT PATCH
205403	MS02-054: Unchecked Buffer in File Decompression Functions Could Lead to Code Execution - Windows ME
205404	MS02-054: Unchecked Buffer in File Decompression Functions Could Lead to Code Execution - Windows ME - CORRUPT PATCH
205405	MS02-054: Unchecked Buffer in File Decompression Functions Could Lead to Code Execution - Windows 98 Plus
205501	MS02-055: Unchecked Buffer in Windows Help Facility - Windows 98
205502	MS02-055: Unchecked Buffer in Windows Help Facility - Windows ME
205505	MS02-055: Unchecked Buffer in Windows Help Facility - Windows 2000
205506	MS02-055: Unchecked Buffer in Windows Help Facility - Windows XP
205507	MS02-055: Unchecked Buffer in Windows Help Facility - Windows 2000 - CORRUPT PATCH
205508	MS02-055: Unchecked Buffer in Windows Help Facility - Windows XP - CORRUPT PATCH
206001	MS02-060: Flaw in Windows XP Help and Support Center
206301	MS02-063: Unchecked Buffer in PPTP Implementation - Windows 2000
206302	MS02-063: Unchecked Buffer in PPTP Implementation - Windows 2000 - CORRUPT PATCH
206303	MS02-063: Unchecked Buffer in PPTP Implementation - Windows XP Gold
206305	MS02-063: Unchecked Buffer in PPTP Implementation - Windows XP SP1

206703	MS02-067: Processing Flaw Could Cause Outlook 2002 to Fail - Windows NT/2000/XP (Administrative Installation)
207001	MS02-070: Flaw in SMB Signing Could Enable Group Policy to be Modified - Windows XP
207002	MS02-070: Flaw in SMB Signing Could Enable Group Policy to be Modified - Windows XP - CORRUPT PATCH
300601	MS03-006: Flaw in Windows ME Help and Support Center
300602	MS03-006: Flaw in Windows ME Help and Support Center - CORRUPT PATCH
300801	MS03-008: Flaw in Windows Script Engine 5.6 Could Allow Code Execution - Windows XP / Windows 2000
300805	MS03-008: Flaw in Windows Script Engine 5.6 Could Allow Code Execution - Windows NT / Windows 98 / Windows ME
300811	MS03-008: Flaw in Windows Script Engine 5.1 Could Allow Code Execution - Windows 2000
300812	MS03-008: Flaw in Windows Script Engine 5.1 Could Allow Code Execution - Windows NT / Windows 98 / Windows ME
300817	MS03-008: Flaw in Windows Script Engine 5.5 Could Allow Code Execution - Windows 2000
300818	MS03-008: Flaw in Windows Script Engine 5.5 Could Allow Code Execution - Windows NT / Windows 98 / Windows ME
301005	MS03-010: RPC Endpoint Mapper Flaw Could Result in Denial of Service - Windows NT
301701	MS03-017: Flaw with Skins in Windows Media Player 7.1
301703	MS03-017: Flaw with Skins in Windows Media Player 8.0 - Windows XP
301901	MS03-019: Flaw in ISAPI Extension for Windows Media Services Could Cause Denial of Service - Windows 2000
301903	MS03-019: Flaw in ISAPI Extension for Windows Media Services Could Cause Denial of Service - Windows NT
302310	MS03-023: Buffer Overrun In HTML Converter Could Allow Code Execution - Windows ME
302311	MS03-023: Buffer Overrun In HTML Converter Could Allow Code Execution - Windows ME - CORRUPT PATCH
303001	MS03-030: Unchecked Buffer in DirectX Could Enable System Compromise - DirectX 5.2, 6.1, 7.0a
303011	MS03-030: Unchecked Buffer in DirectX Could Enable System Compromise - Windows NT
303012	MS03-030: Unchecked Buffer in DirectX Could Enable System Compromise - Windows NT - CORRUPT PATCH
303013	MS03-030: Unchecked Buffer in DirectX Could Enable System Compromise - Windows NT TSE
303014	MS03-030: Unchecked Buffer in DirectX Could Enable System Compromise - Windows NT TSE - CORRUPT PATCH

303015	MS03-030: Unchecked Buffer in DirectX Could Enable System Compromise - DirectX 8.0 - 8.1b on Windows 2000 SP3
303017	MS03-030: Unchecked Buffer in DirectX Could Enable System Compromise - DirectX 8.0 - 8.1b on Windows 2000 SP3 - CORRUPT PATCH
303602	MS03-036: Buffer Overrun in WordPerfect Converter Could Allow Code Execution - Office XP Applications - Windows 95/98/ME (Administrative Installation)
303603	MS03-036: Buffer Overrun in WordPerfect Converter Could Allow Code Execution - Office XP Applications - Windows 2000/NT/XP (Administrative Installation)
303608	MS03-036: Buffer Overrun in WordPerfect Converter Could Allow Code Execution - Office 2000 Applications - Windows 2000/NT/XP (Administrative Installation)
303802	MS03-038: Unchecked Buffer in Microsoft Access Could Allow Code Execution - Access 2002 on Windows 2000/NT/XP (Administrative Installation)
303803	MS03-038: Unchecked Buffer in Microsoft Access Could Allow Code Execution - Access 2002 on Windows 98/ME (Administrative Installation)
400902	MS04-009: Vulnerability in Microsoft Outlook 2002 Could Allow Code Execution - Windows NT/2000/XP (Administrative Installation)
401201	MS04-012: Cumulative Update for Microsoft RPC/DCOM - Windows 2000
401202	MS04-012: Cumulative Update for Microsoft RPC/DCOM - Windows 2000 - CORRUPT PATCH
401301	MS04-013: Cumulative Security Update for Outlook Express 6.0 SP1
401302	MS04-013: Cumulative Security Update for Outlook Express 6.0 SP1 - CORRUPT PATCH
401407	MS04-014: Vulnerability in the Microsoft Jet Database Engine Could Allow Code Execution - Windows NT
401607	MS04-016: Vulnerability in DirectX Could Allow Denial of Service - DirectX 8.1 on Windows 2000
401608	MS04-016: Vulnerability in DirectX Could Allow Denial of Service - DirectX 8.1 on Windows 2000 - CORRUPT PATCH
401609	MS04-016: Vulnerability in DirectX Could Allow Denial of Service - DirectX 8.2 on Windows 2000
401610	MS04-016: Vulnerability in DirectX Could Allow Denial of Service - DirectX 8.2 on Windows 2000 - CORRUPT PATCH
401611	MS04-016: Vulnerability in DirectX Could Allow Denial of Service - DirectX 8.0 on Windows 2000
401612	MS04-016: Vulnerability in DirectX Could Allow Denial of Service - DirectX 8.0 on Windows 2000 - CORRUPT PATCH

401613	MS04-016: Vulnerability in DirectX Could Allow Denial of Service - DirectX 9.0 on Windows 2000/XP/2003
401614	MS04-016: Vulnerability in DirectX Could Allow Denial of Service - DirectX 9.0 on Windows 2000/XP/2003 - CORRUPT PATCH
401803	MS04-018: Vulnerability in Outlook Express - IE 5.5 SP2, IE 5.01 SP3
401804	MS04-018: Vulnerability in Outlook Express - IE 5.5 SP2, IE 5.01 SP3 - CORRUPT PATCH
401807	MS04-018: Vulnerability in Outlook Express - IE 6 SP1
401808	MS04-018: Vulnerability in Outlook Express - IE 6 SP1 - CORRUPT PATCH
402702	MS04-027: Vulnerability in WordPerfect Converter Could Allow Code Execution - Office 2000 - Windows NT/2000/XP (Administrative Installation)
402705	MS04-027: Vulnerability in WordPerfect Converter Could Allow Code Execution - Office XP - Windows NT/2000/XP (Administrative Installation)
402706	MS04-027: Vulnerability in WordPerfect Converter Could Allow Code Execution - Office XP - Windows 9x/ME (Administrative Installation)
402815	MS04-028: Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution - Visual Studio .NET 2002
402832	MS04-028: Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution - FoxPro 8.0 - Windows 2000
403211	MS04-032: Security Update for Windows Kernel - Windows NT Server (Large System Partition)
403212	MS04-032: Security Update for Windows Kernel - Windows NT Terminal Server (Large System Partition)
403213	MS04-032: Security Update for Windows Kernel - Windows NT Server (Large System Partition) - CORRUPT PATCH
403214	MS04-032: Security Update for Windows Kernel - Windows NT Terminal Server (Large System Partition) - CORRUPT PATCH
403302	MS04-033: Vulnerability in Microsoft Excel Could Allow Remote Code Execution - Office XP - Windows NT/2000/XP/2003 (Administrative Installation)
403303	MS04-033: Vulnerability in Microsoft Excel Could Allow Remote Code Execution - Office XP - Windows 95/98/ME (Administrative Installation)
403606	MS04-036: Vulnerability in NNTP Could Allow Remote Code Execution - Windows NT Server 4.0 - CORRUPT PATCH
403703	MS04-037: Vulnerability in Windows Shell Could Allow Remote Code Execution - Windows 2000
403704	MS04-037: Vulnerability in Windows Shell Could Allow Remote Code Execution - Windows 2000 - CORRUPT PATCH
403903	MS04-039: Vulnerability Could Allow Internet Content Spoofing - Proxy Server 2.0

404411	MS04-044: Vulnerabilities in Windows Kernel and LSASS Could Allow Elevation of Privilege - Windows NT Server (Large System Partition)
404412	MS04-044: Vulnerabilities in Windows Kernel and LSASS Could Allow Elevation of Privilege - Windows NT Terminal Server (Large System Partition)
404413	MS04-044: Vulnerabilities in Windows Kernel and LSASS Could Allow Elevation of Privilege - Windows NT Server (Large System Partition) - CORRUPT PATCH
404414	MS04-044: Vulnerabilities in Windows Kernel and LSASS Could Allow Elevation of Privilege - Windows NT Terminal Server (Large System Partition) - CORRUPT PATCH
452001	UPDATE: Microsoft .NET Framework 4.5.2 Available - Windows Vista SP2 / Windows 7 SP1 / Windows 8 / Windows 8.1 / Windows Server 2008 SP2 / Windows Server 2008 R2 SP1 / Windows Server 2012 / Windows Server 2012 R2
500211	MS05-002: Vulnerability in Cursor and Icon Format Handling Could Allow Remote Code Execution - Windows 98 (v2, re-released 4/12/2005)
500212	MS05-002: Vulnerability in Cursor and Icon Format Handling Could Allow Remote Code Execution - Windows 98 (v2, re-released 4/12/2005) - CORRUPT PATCH
500213	MS05-002: Vulnerability in Cursor and Icon Format Handling Could Allow Remote Code Execution - Windows ME (v2, re-released 4/12/2005)
500214	MS05-002: Vulnerability in Cursor and Icon Format Handling Could Allow Remote Code Execution - Windows ME (v2, re-released 4/12/2005) - CORRUPT PATCH
500401	MS05-004: Vulnerability in ASP.NET Path Validation - .NET Framework 1.0 SP3 - Windows 2000 SP3 / XP SP1
500402	MS05-004: Vulnerability in ASP.NET Path Validation - .NET Framework 1.0 SP3 - Windows 2000/XP/2003 - CORRUPT PATCH
500403	MS05-004: Vulnerability in ASP.NET Path Validation - .NET Framework 1.0 SP2 - Windows 2000/XP/2003
500404	MS05-004: Vulnerability in ASP.NET Path Validation - .NET Framework 1.0 SP2 - Windows 2000/XP/2003 - CORRUPT PATCH
500405	MS05-004: Vulnerability in ASP.NET Path Validation - .NET Framework 1.1 SP1 - Windows 2000/XP
500406	MS05-004: Vulnerability in ASP.NET Path Validation - .NET Framework 1.1 SP1 - Windows 2000/XP - CORRUPT PATCH
500409	MS05-004: Vulnerability in ASP.NET Path Validation - .NET Framework 1.1 - Windows 2000/XP
500410	MS05-004: Vulnerability in ASP.NET Path Validation - .NET Framework 1.1 - Windows 2000/XP - CORRUPT PATCH

500901	MS05-009: Vulnerability in PNG Processing Could Allow Remote Code Execution - Windows Media Player 9 Series
500904	MS05-009: Vulnerability in PNG Processing Could Allow Remote Code Execution - Windows Messenger 4.7.0.2009 on Windows XP SP1
500906	MS05-009: Vulnerability in PNG Processing Could Allow Remote Code Execution - Windows Messenger 4.7.0.3000 on Windows XP SP2
500907	MS05-009: Vulnerability in PNG Processing Could Allow Remote Code Execution - Windows Messenger 4.7.0.3000 on Windows XP SP2 - CORRUPT PATCH
501307	MS05-013: Vulnerability in the DHTML Editing Component ActiveX Control Could Allow Remote Code Execution - Windows 98/ME
501308	MS05-013: Vulnerability in the DHTML Editing Component ActiveX Control Could Allow Remote Code Execution - Windows 98/ME - CORRUPT PATCH
501507	MS05-015: Vulnerability in Hyperlink Object Library Could Allow Remote Code Execution - Windows 98!Win98!Tue, 08 Feb 200
501508	MS05-015: Vulnerability in Hyperlink Object Library Could Allow Remote Code Execution - Windows 98 - CORRUPT PATCH
501509	MS05-015: Vulnerability in Hyperlink Object Library Could Allow Remote Code Execution - Windows ME
501510	MS05-015: Vulnerability in Hyperlink Object Library Could Allow Remote Code Execution - Windows ME - CORRUPT PATCH
502607	MS05-026: Vulnerability in HTML Help Could Allow Remote Code Execution - Windows ME
502608	MS05-026: Vulnerability in HTML Help Could Allow Remote Code Execution - Windows ME - CORRUPT PATCH
502609	MS05-026: Vulnerability in HTML Help Could Allow Remote Code Execution - Windows 98
502610	MS05-026: Vulnerability in HTML Help Could Allow Remote Code Execution - Windows 98 - CORRUPT PATCH
502614	MS05-026: Vulnerability in HTML Help Could Allow Remote Code Execution - Windows XP/2003 (x64)
502615	MS05-026: Vulnerability in HTML Help Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
502708	MS05-027: Vulnerability in Server Message Block Could Allow Remote Code Execution - Windows XP/2003 (x64)
502709	MS05-027: Vulnerability in Server Message Block Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
503001	MS05-030: Security Update for Outlook Express - OE 5.5 SP2 for Windows 2000
503002	MS05-030: Security Update for Outlook Express - OE 5.5 SP2 for Windows 2000 - CORRUPT PATCH

503005	MS05-030: Security Update for Outlook Express - OE 6.0 SP1 for Windows 2000/XP
503006	MS05-030: Security Update for Outlook Express - OE 6.0 SP1 for Windows 2000/XP - CORRUPT PATCH
503104	MS05-031: Vulnerability in Step-by-Step Interactive Training Could Allow Remote Code Execution - Windows XP/2003 (x64)
503105	MS05-031: Vulnerability in Step-by-Step Interactive Training Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
503208	MS05-032: Security Update for MSAgent ActiveX - Windows XP/2003 (x64)
503209	MS05-032: Security Update for MSAgent ActiveX - Windows XP/2003 (x64) - CORRUPT PATCH
503316	MS05-033: Security Update for Telnet - Windows XP/2003 (x64)
503317	MS05-033: Security Update for Telnet - Windows XP/2003 (x64) - CORRUPT PATCH
503608	MS05-036: Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution - Windows XP/2003 (x64)
503609	MS05-036: Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
503908	MS05-039: Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege - Windows XP/2003 (x64)
503909	MS05-039: Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege - Windows XP/2003 (x64) - CORRUPT PATCH
504008	MS05-040: Vulnerability in Telephony Service Could Allow Remote Code Execution - Windows XP/2003 (x64)
504009	MS05-040: Vulnerability in Telephony Service Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
504108	MS05-041: Vulnerability in Remote Desktop Protocol Could Allow Denial of Service - Windows XP/2003 (x64)
504109	MS05-041: Vulnerability in Remote Desktop Protocol Could Allow Denial of Service - Windows XP/2003 (x64) - CORRUPT PATCH
504208	(MS05-042: Vulnerabilities in Kerberos Could Allow Denial of Service
504209	(MS05-042: Vulnerabilities in Kerberos Could Allow Denial of Service
504810	MS05-048: Vulnerability in the Microsoft Collaboration Data Objects Could Allow Remote Code Execution - Windows XP/2003 (x64)
504811	MS05-048: Vulnerability in the Microsoft Collaboration Data Objects Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
504902	MS05-049: Vulnerabilities in Windows Shell Could Allow Remote Code Execution - Windows XP/2003 (x64)

504909	MS05-049: Vulnerabilities in Windows Shell Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
505011	MS05-050: Vulnerability in DirectShow Could Allow Remote Code Execution - DirectX 9.0 on Windows XP SP1
505012	MS05-050: Vulnerability in DirectShow Could Allow Remote Code Execution - DirectX 9.0 on Windows XP SP1 - CORRUPT PATCH
505017	MS05-050: Vulnerability in DirectShow Could Allow Remote Code Execution - DirectX 8.0/8.1/8.2 on Windows 98/ME
505018	MS05-050: Vulnerability in DirectShow Could Allow Remote Code Execution - DirectX 8.0/8.1/8.2 on Windows 98/ME - CORRUPT PATCH
505019	MS05-050: Vulnerability in DirectShow Could Allow Remote Code Execution - DirectX 9.0 on Windows 98/ME
505020	MS05-050: Vulnerability in DirectShow Could Allow Remote Code Execution - DirectX 9.0 on Windows 98/ME - CORRUPT PATCH
505021	MS05-050: Vulnerability in DirectShow Could Allow Remote Code Execution - Windows XP SP1 (v2
505022	MS05-050: Vulnerability in DirectShow Could Allow Remote Code Execution - Windows XP SP1 (v2
505108	MS05-051: Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution - Windows XP/2003 (x64)
505109	MS05-051: Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
505411	MS05-054: Cumulative Security Update for Internet Explorer - IE 5.5 SP2 - Windows ME
505412	MS05-054: Cumulative Security Update for Internet Explorer - IE 5.5 SP2 - Windows ME - CORRUPT PATCH
600103	MS06-001: Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution - Windows XP SP1
600104	MS06-001: Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution - Windows XP SP1 - CORRUPT PATCH
600201	MS06-002: Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution - Windows XP SP1
600202	MS06-002: Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution - Windows XP SP1 - CORRUPT PATCH
600208	MS06-002: Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution - Windows XP/2003 (x64)
600209	MS06-002: Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution - Windows 98
600210	MS06-002: Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution - Windows 98 - CORRUPT PATCH
600211	MS06-002: Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution - Windows ME

600212	MS06-002: Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution - Windows ME - CORRUPT PATCH
600213	MS06-002: Vulnerability in Embedded Web Fonts Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
600601	MS06-006: Vulnerability in Windows Media Player Plug-in with Non-Microsoft Internet Browsers Could Allow Remote Code Execution - Windows 2000/XP/2003
600602	MS06-006: Vulnerability in Windows Media Player Plug-in with Non-Microsoft Internet Browsers Could Allow Remote Code Execution - Windows 2000/XP/2003 - CORRUPT PATCH
600604	MS06-006: Vulnerability in Windows Media Player Plug-in with Non-Microsoft Internet Browsers Could Allow Remote Code Execution - Windows XP/2003 (x64)
600605	MS06-006: Vulnerability in Windows Media Player Plug-in with Non-Microsoft Internet Browsers Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
600803	MS06-008: Vulnerability in Web Client Service Could Allow Remote Code Execution - Windows XP SP1/SP2
600804	MS06-008: Vulnerability in Web Client Service Could Allow Remote Code Execution - Windows XP SP1/SP2 - CORRUPT PATCH
600806	MS06-008: Vulnerability in Web Client Service Could Allow Remote Code Execution - Windows XP/2003 (x64)
600807	MS06-008: Vulnerability in Web Client Service Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
600901	MS06-009: Vulnerability in the Korean IME Could Allow Elevation of Privilege - Windows XP SP1/SP2
600902	MS06-009: Vulnerability in the Korean IME Could Allow Elevation of Privilege - Windows XP SP1/SP2 - CORRUPT PATCH
600931	MS06-009: Vulnerability in the Korean IME Could Allow Elevation of Privilege - Windows XP/2003 (x64)
600932	MS06-009: Vulnerability in the Korean IME Could Allow Elevation of Privilege - Windows XP/2003 (x64) - CORRUPT PATCH
601201	MS06-012: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution - Outlook 2000 (Local Installation)
601202	MS06-012: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution - Outlook 2000 - Windows NT/2000/XP/2003 (Network Installation)
601204	MS06-012: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution - Outlook 2000 - Windows NT/2000/XP/2003 (Administrative Installation)
601219	MS06-012: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution - PowerPoint 2000 - Windows NT/2000/XP/2003 (Administrative Installation)

601251	MS06-012: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution - PowerPoint 2002 - Windows NT/2000/XP/2003 (Administrative Installation)
601401	MS06-014: Vulnerability in the MDAC Function Could Allow Code Execution - Windows XP SP1/SP2
601402	MS06-014: Vulnerability in the MDAC Function Could Allow Code Execution - Windows XP SP1/SP2 - CORRUPT PATCH
601413	MS06-014: Vulnerability in the MDAC Function Could Allow Code Execution - Windows XP/2003 (x64)
601414	MS06-014: Vulnerability in the MDAC Function Could Allow Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
601417	MS06-014: Vulnerability in the MDAC Function Could Allow Code Execution - MDAC 2.80 - Windows 98/ME
601418	MS06-014: Vulnerability in the MDAC Function Could Allow Code Execution - MDAC 2.80 - Windows 98/ME - CORRUPT PATCH
601419	MS06-014: Vulnerability in the MDAC Function Could Allow Code Execution - MDAC 2.81 - Windows 98/ME
601420	MS06-014: Vulnerability in the MDAC Function Could Allow Code Execution - MDAC 2.81 - Windows 98/ME - CORRUPT PATCH
601514	MS06-015: Vulnerability in Windows Explorer Could Allow Remote Code Execution - Windows Server 2003 (v2
601515	MS06-015: Vulnerability in Windows Explorer Could Allow Remote Code Execution - Windows Server 2003 (v2
601516	MS06-015: Vulnerability in Windows Explorer Could Allow Remote Code Execution - Windows XP/2003 (x64) (v2
601517	MS06-015: Vulnerability in Windows Explorer Could Allow Remote Code Execution - Windows XP/2003 (x64) (v2
602112	MS06-021: Cumulative Security Update for Internet Explorer - IE 6.0 SP1 - Windows 98/ME
602113	MS06-021: Cumulative Security Update for Internet Explorer - IE 6.0 SP1 - Windows 98/ME - CORRUPT PATCH
602203	MS06-022: Vulnerability in ART Image Rendering Could Allow Remote Code Execution - Windows XP SP2
602204	MS06-022: Vulnerability in ART Image Rendering Could Allow Remote Code Execution - Windows XP SP2 - CORRUPT PATCH
602212	MS06-022: Vulnerability in ART Image Rendering Could Allow Remote Code Execution - IE 6.0 SP1 - Windows 98/ME
602213	MS06-022: Vulnerability in ART Image Rendering Could Allow Remote Code Execution - IE 6.0 SP1 - Windows 98/ME - CORRUPT PATCH
602302	MS06-023: Vulnerability in Microsoft JScript Could Allow Remote Code Execution - Windows XP SP1
602306	MS06-023: Vulnerability in Microsoft JScript Could Allow Remote Code Execution - Windows XP SP1 - CORRUPT PATCH

602308	MS06-023: Vulnerability in Microsoft JScript Could Allow Remote Code Execution - Windows 98/ME
602415	MS06-024: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Windows Media Player 9 - Windows 98
602416	MS06-024: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Windows Media Player 9 - Windows 98 - CORRUPT PATCH
602417	MS06-024: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Windows ME
602418	MS06-024: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Windows ME - CORRUPT PATCH
602527	MS06-025: Vulnerability in Routing and Remote Access Could Allow Remote Code Execution - Windows XP/2003 (x64) (v2
602528	MS06-025: Vulnerability in Routing and Remote Access Could Allow Remote Code Execution - Windows XP/2003 (x64) (v2
602601	MS06-026: Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution - Windows 98
602602	MS06-026: Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution - Windows 98 - CORRUPT PATCH
602603	MS06-026: Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution - Windows ME
602604	MS06-026: Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution - Windows ME - CORRUPT PATCH
603007	MS06-030: Vulnerability in Server Message Block Could Allow Elevation of Privilege - Windows XP/2003 (x64)
603008	MS06-030: Vulnerability in Server Message Block Could Allow Elevation of Privilege - Windows XP/2003 (x64) - CORRUPT PATCH
603607	MS06-036: Vulnerability in DHCP Client Service Could Allow Remote Code Execution - Windows XP/2003 (x64)
603608	MS06-036: Vulnerability in DHCP Client Service Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
603917	MS06-039: Vulnerabilities in Microsoft Office Filters Could Allow Remote Code Execution - Project 2000 (Network/Local Installation)
604107	MS06-041: Vulnerability in DNS Resolution Could Allow Remote Code Execution - Windows XP/2003 (x64)
604108	MS06-041: Vulnerability in DNS Resolution Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
604607	MS06-046: Vulnerability in HTML Help Could Allow Remote Code Execution - Windows XP/2003 (x64)
604608	MS06-046: Vulnerability in HTML Help Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
605007	MS06-050: Vulnerabilities in Microsoft Windows Hyperlink Object Library Could Allow Remote Code Execution - Windows XP/2003 (x64)

605008	MS06-050: Vulnerabilities in Microsoft Windows Hyperlink Object Library Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
605307	MS06-053: Vulnerability in Indexing Service Could Allow Cross-Site Scripting - Windows XP/2003 (x64)
605309	MS06-053: Vulnerability in Indexing Service Could Allow Cross-Site Scripting - Windows XP/2003 (x64) - CORRUPT PATCH
605601	MS06-056: Vulnerability in ASP.NET 2.0 Could Allow Information Disclosure - Windows 2000/XP/2003
605602	MS06-056: Vulnerability in ASP.NET 2.0 Could Allow Information Disclosure - Windows 2000/XP/2003 - CORRUPT PATCH
605607	MS06-056: Vulnerability in ASP.NET 2.0 Could Allow Information Disclosure - Windows XP/2003 (x64)
605608	MS06-056: Vulnerability in ASP.NET 2.0 Could Allow Information Disclosure - Windows XP/2003 (x64) - CORRUPT PATCH
605703	MS06-057: Vulnerability in Windows Explorer Could Allow Remote Execution - Windows Server 2003
605704	MS06-057: Vulnerability in Windows Explorer Could Allow Remote Execution - Windows Server 2003 - CORRUPT PATCH
605707	MS06-057: Vulnerability in Windows Explorer Could Allow Remote Execution - Windows XP/2003 (x64)
605710	MS06-057: Vulnerability in Windows Explorer Could Allow Remote Execution - Windows XP/2003 (x64) - CORRUPT PATCH
606807	MS06-068: Vulnerability in Microsoft Agent Could Allow Remote Code Execution - Windows XP/2003 (x64)
606808	MS06-068: Vulnerability in Microsoft Agent Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
607407	MS06-074: Vulnerability in SNMP Could Allow Remote Code Execution - Windows XP/2003 (x64)
607408	MS06-074: Vulnerability in SNMP Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
607601	MS06-076: Cumulative Security Update for Outlook Express - Windows Server 2003
607602	MS06-076: Cumulative Security Update for Outlook Express - Windows Server 2003 - CORRUPT PATCH
607807	MS06-078: Vulnerability in Windows Media Format Could Allow Remote Code Execution - Windows XP/2003 (x64)
607808	MS06-078: Vulnerability in Windows Media Format Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
700505	MS07-005: Vulnerability in Step-by-Step Interactive Training Could Allow Remote Code Execution - Windows XP/2003 (x64)

700506	MS07-005: Vulnerability in Step-by-Step Interactive Training Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
700605	MS07-006: Vulnerability in Windows Shell Could Allow Elevation of Privilege - Windows XP/2003 (x64)
700606	MS07-006: Vulnerability in Windows Shell Could Allow Elevation of Privilege - Windows XP/2003 (x64) - CORRUPT PATCH
700807	MS07-008: Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution - Windows XP/2003 (x64)
700808	MS07-008: Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
701005	MS07-010: Vulnerability in Microsoft Malware Protection Engine Could Allow Remote Code Execution - Windows Defender - Windows XP/2003 (x64)
701006	MS07-010: Vulnerability in Microsoft Malware Protection Engine Could Allow Remote Code Execution - ForeFront Security for Exchange Server 10 - Windows XP/2003 (x64)
701107	MS07-011: Vulnerability in Microsoft OLE Dialog Could Allow Remote Code Execution - Windows XP/2003 (x64)
701110	MS07-011: Vulnerability in Microsoft OLE Dialog Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
701220	MS07-012: Vulnerability in Microsoft MFC Could Allow Remote Code Execution - Windows XP/2003 (x64) (v2
701304	MS07-013: Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution - Office 2000 - Windows NT/2000/XP/2003 (Administrative Installation)
701307	MS07-013: Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution - Office XP - Windows NT/2000/XP/2003 (Administrative Installation)
701308	MS07-013: Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution - Office XP - 9x/ME (Administrative Installation)
701313	MS07-013: Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution - Windows 2000 SP4
701314	MS07-013: Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution - Windows 2000 SP4 - CORRUPT PATCH
701319	MS07-013: Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution - Windows XP/2003 (x64)
701320	MS07-013: Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
701617	MS07-016: Cumulative Security Update for Internet Explorer - IE 6.0 - Windows Server 2003
701618	MS07-016: Cumulative Security Update for Internet Explorer - IE 6.0 - Windows Server 2003 - CORRUPT PATCH

701701	MS07-017: Vulnerabilities in GDI Could Allow Remote Code Execution - Windows XP/2003 (x64)
701702	MS07-017: Vulnerabilities in GDI Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
701709	MS07-017: Vulnerabilities in GDI Could Allow Remote Code Execution - Windows Vista
701711	MS07-017: Vulnerabilities in GDI Could Allow Remote Code Execution - Windows Vista (x64)
701805	MS07-018: Vulnerabilities in Microsoft Content Management Server Could Allow Remote Code Execution - MCMS 2001 SP1 - Windows XP/2003
701901	MS07-019: Vulnerability in Universal Plug and Play Could Allow Remote Code Execution - Windows XP (x64)
701902	MS07-019: Vulnerability in Universal Plug and Play Could Allow Remote Code Execution - Windows XP (x64) - CORRUPT PATCH
702001	MS07-020: Vulnerability in Microsoft Agent Could Allow Remote Code Execution - Windows XP/2003 (x64)
702002	MS07-020: Vulnerability in Microsoft Agent Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
702101	MS07-021: Vulnerabilities in CSRSS Could Allow Remote Code Execution - Windows XP/2003 Gold (x64)
702102	MS07-021: Vulnerabilities in CSRSS Could Allow Remote Code Execution - Windows XP/2003 Gold (x64) - CORRUPT PATCH
702109	MS07-021: Vulnerabilities in CSRSS Could Allow Remote Code Execution - Windows Vista
702111	MS07-021: Vulnerabilities in CSRSS Could Allow Remote Code Execution - Windows Vista (x64)
703201	MS07-032: Vulnerability in Windows Vista Could Allow Information Disclosure - Windows Vista
703203	MS07-032: Vulnerability in Windows Vista Could Allow Information Disclosure - Windows Vista (x64)
703403	MS07-034: Cumulative Security Update for Outlook Express and Windows Mail - Windows 2003 SP1/SP2
703405	MS07-034: Cumulative Security Update for Outlook Express and Windows Mail - Windows XP/2003 (x64)
703406	MS07-034: Cumulative Security Update for Outlook Express and Windows Mail - Windows 2003 SP1/SP2 - CORRUPT PATCH
703408	MS07-034: Cumulative Security Update for Outlook Express and Windows Mail - Windows XP/2003 (x64) - CORRUPT PATCH
703411	MS07-034: Cumulative Security Update for Outlook Express and Windows Mail - Windows Vista
703413	MS07-034: Cumulative Security Update for Outlook Express and Windows Mail - Windows Vista (x64)

703803	MS07-038: Vulnerability in Windows Vista Firewall Could Allow Information Disclosure - Windows Vista (v2, re-released 8/14/2007)
703804	MS07-038: Vulnerability in Windows Vista Firewall Could Allow Information Disclosure - Windows Vista (x64) (v2, re-released 8/14/2007)
704003	MS07-040: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 1.0 SP3 - Windows 2000/XP/2003/Vista/2008
704004	MS07-040: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 1.0 SP3 - Windows 2000/XP/2003/Vista/2008 - CORRUPT PATCH
704007	MS07-040: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 1.0 SP3 - Windows XP/2003 (x64)
704008	MS07-040: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 1.0 SP3 - Windows XP/2003 (x64) - CORRUPT PATCH
704009	MS07-040: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 2.0 - Windows 2000/XP/2003
704010	MS07-040: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 2.0 - Windows 2000/XP/2003 - CORRUPT PATCH
704011	MS07-040: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 2.0 - Windows Vista
704019	MS07-040: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 2.0 - Windows Vista (x64)
704021	MS07-040: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 2.0 - Windows XP/2003 (x64)
704022	MS07-040: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 2.0 - Windows XP/2003 (x64) - CORRUPT PATCH
704023	MS07-040: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 1.1 SP1 - Windows XP/2003 (x64)
704024	MS07-040: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 1.1 SP1 - Windows XP/2003 (x64) - CORRUPT PATCH
704713	MS07-047: Vulnerabilities in Windows Media Player Could Allow Remote Code Execution - Windows Media Player 10 - Windows XP/2003 (x64)
704714	MS07-047: Vulnerabilities in Windows Media Player Could Allow Remote Code Execution - Windows Media Player 10 - Windows XP/2003 (x64) - CORRUPT PATCH
704717	MS07-047: Vulnerabilities in Windows Media Player Could Allow Remote Code Execution - Windows Media Player 11 - Windows XP (x64)

704718	MS07-047: Vulnerabilities in Windows Media Player Could Allow Remote Code Execution - Windows Media Player 11 - Windows XP (x64) - CORRUPT PATCH
704801	MS07-048: Vulnerabilities in Windows Gadgets Could Allow Remote Code Execution - Windows Vista
704803	MS07-048: Vulnerabilities in Windows Gadgets Could Allow Remote Code Execution - Windows Vista (x64)
705005	MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code Execution - IE 6 - Windows XP SP2
705006	MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code Execution - IE 6 - Windows XP SP2 - CORRUPT PATCH
705013	MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code Execution - IE 7 - Windows Vista
705014	MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code Execution - IE 7 - Windows XP SP2 (v2
705015	MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code Execution - IE 6 - Windows XP/2003 (x64)
705016	MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code Execution - IE 6 - Windows XP/2003 (x64) - CORRUPT PATCH
705017	MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code Execution - IE 7 - Windows XP/2003 (x64)
705018	MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code Execution - IE 7 - Windows XP/2003 (x64) - CORRUPT PATCH
705019	MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code Execution - IE 7 - Windows Vista (x64)
705020	MS07-050: Vulnerability in Vector Markup Language Could Allow Remote Code Execution - IE 7 - Windows XP SP2 (v2
705307	MS07-053: Vulnerability in Subsystem for UNIX-based Applications Could Allow Elevation of Privilege - Windows Vista
705311	MS07-053: Vulnerability in Subsystem for UNIX-based Applications Could Allow Elevation of Privilege - Windows Vista (x64)
705401	MS07-054: Vulnerability in MSN Messenger and Windows Live Messenger Could Allow Remote Code Execution - MSN Messenger 6.2/7.0 - Windows 2000 SP4
705403	MS07-054: Vulnerability in MSN Messenger and Windows Live Messenger Could Allow Remote Code Execution - MSN Messenger 6.2/7.0/7.5/8.0 - Windows XP/2003/Vista
705407	MS07-054: Vulnerability in MSN Messenger and Windows Live Messenger Could Allow Remote Code Execution - MSN Messenger 6.2/7.0/7.5/8.0 - Windows XP/2003/Vista (x64)

705805	MS07-058: Vulnerability in RPC Could Allow Denial of Service - Windows XP Gold (x64)
705806	MS07-058: Vulnerability in RPC Could Allow Denial of Service - Windows XP Gold (x64) - CORRUPT PATCH
706103	MS07-061: Vulnerability in Windows URI Handling Could Allow Remote Code Execution - Windows XP Gold (x64)
706104	MS07-061: Vulnerability in Windows URI Handling Could Allow Remote Code Execution - Windows XP Gold (x64) - CORRUPT PATCH
706301	MS07-063: Vulnerability in SMBv2 Could Allow Remote Code Execution - Windows Vista
706303	MS07-063: Vulnerability in SMBv2 Could Allow Remote Code Execution - Windows Vista (x64)
706703	MS07-067: Vulnerability in Macrovision Driver Could Allow Local Elevation of Privilege - Windows XP (x64)
706704	MS07-067: Vulnerability in Macrovision Driver Could Allow Local Elevation of Privilege - Windows XP (x64) - CORRUPT PATCH
706805	MS07-068: Vulnerability in Windows Media File Format Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 - Windows XP/2003 (x64)
706806	MS07-068: Vulnerability in Windows Media File Format Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 - Windows XP/2003 (x64) - CORRUPT PATCH
706811	MS07-068: Vulnerability in Windows Media File Format Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 x64 Edition - Windows XP/2003 (x64)
706812	MS07-068: Vulnerability in Windows Media File Format Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 x64 Edition - Windows XP/2003 (x64) - CORRUPT PATCH
706813	MS07-068: Vulnerability in Windows Media File Format Could Allow Remote Code Execution - Windows Media Format Runtime 11 - Windows XP (x64)
706814	MS07-068: Vulnerability in Windows Media File Format Could Allow Remote Code Execution - Windows Media Format Runtime 11 - Windows XP (x64) - CORRUPT PATCH
706815	MS07-068: Vulnerability in Windows Media File Format Could Allow Remote Code Execution - Windows Media Format Runtime 11 - Windows Vista
706817	MS07-068: Vulnerability in Windows Media File Format Could Allow Remote Code Execution - Windows Media Format Runtime 11 - Windows Vista (x64)
800401	MS08-004: Vulnerability in Windows TCP/IP Could Allow Denial of Service - Windows Vista
800403	MS08-004: Vulnerability in Windows TCP/IP Could Allow Denial of Service - Windows Vista (x64)

800505	MS08-005: Vulnerability in Internet Information Services Could Allow Elevation of Privilege - Windows XP (x64)
800506	MS08-005: Vulnerability in Internet Information Services Could Allow Elevation of Privilege - Windows XP (x64) - CORRUPT PATCH
800511	MS08-005: Vulnerability in Internet Information Services Could Allow Elevation of Privilege - Windows Vista
800513	MS08-005: Vulnerability in Internet Information Services Could Allow Elevation of Privilege - Windows Vista (x64)
800603	MS08-006: Vulnerability in Internet Information Services Could Allow Remote Code Execution - Windows XP Gold (x64)
800604	MS08-006: Vulnerability in Internet Information Services Could Allow Remote Code Execution - Windows XP Gold (x64) - CORRUPT PATCH
800703	MS08-007: Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution - Windows XP (x64)
800704	MS08-007: Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution - Windows XP (x64) - CORRUPT PATCH
800709	MS08-007: Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution - Windows Vista
800711	MS08-007: Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution - Windows Vista (x64)
800805	MS08-008: Vulnerability in OLE Automation Could Allow Remote Code Execution - Windows XP (x64)
800806	MS08-008: Vulnerability in OLE Automation Could Allow Remote Code Execution - Windows XP (x64) - CORRUPT PATCH
800811	MS08-008: Vulnerability in OLE Automation Could Allow Remote Code Execution - Windows Vista
800813	MS08-008: Vulnerability in OLE Automation Could Allow Remote Code Execution - Windows Vista (x64)
801303	MS08-013: Vulnerability in Microsoft Office Could Allow Remote Code Execution - Office 2000 - Windows NT/2000/XP/2003 (Network Installation)
801305	MS08-013: Vulnerability in Microsoft Office Could Allow Remote Code Execution - Office 2000 - Windows NT/2000/XP/2003 (Administrative Installation)
801505	MS08-015: Vulnerability in Microsoft Outlook Could Allow Remote Code Execution - Outlook 2000 SP3 - Windows NT/2000/XP 2003 (Admin Installation)
801605	MS08-016: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution - Office 2000 SP3 - Windows NT/2000/XP/2003 (Network Installation)
801609	MS08-016: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution - Office 2000 SP3 - Windows NT/2000/XP/2003 (Administrative Installation)

801641	MS08-016: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution - Office Excel Viewer 2003
801642	MS08-016: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution - Office Word Viewer 2003
801719	MS08-017: Vulnerabilities in Microsoft Office Web Components Could Allow Remote Code Execution - Office 2000 SP3 - Windows NT/2000/XP/2003 (Administrative Installation)
801741	MS08-017: Vulnerabilities in Microsoft Office Web Components Could Allow Remote Code Execution - Commerce Server 2000
802005	MS08-020: Vulnerability in DNS Client Could Allow Spoofing - Windows XP Gold (x64)
802006	MS08-020: Vulnerability in DNS Client Could Allow Spoofing - Windows XP Gold (x64) - CORRUPT PATCH
802011	MS08-020: Vulnerability in DNS Client Could Allow Spoofing - Windows Vista
802013	MS08-020: Vulnerability in DNS Client Could Allow Spoofing - Windows Vista (x64)
802217	MS08-022: Vulnerability in VBScript and JScript Scripting Engines Could Allow Remote Code Execution - Windows XP (x64) (v2
802218	MS08-022: Vulnerability in VBScript and JScript Scripting Engines Could Allow Remote Code Execution - Windows XP (x64) (v2
802703	MS08-027: Vulnerability in Microsoft Publisher Could Allow Remote Code Execution - Office 2000 SP3 - Windows NT/2000/XP/2003 (Network Installation)
802705	MS08-027: Vulnerability in Microsoft Publisher Could Allow Remote Code Execution - Office 2000 SP3 - Windows NT/2000/XP/2003 (Administrative Installation)
802805	MS08-028: Vulnerability in Microsoft Jet Database Engine Could Allow Remote Code Execution - Windows XP (x64)
802806	MS08-028: Vulnerability in Microsoft Jet Database Engine Could Allow Remote Code Execution - Windows XP (x64) - CORRUPT PATCH
803003	MS08-030: Vulnerability in Bluetooth Stack Could Allow Remote Code Execution - Windows XP (x64)
803004	MS08-030: Vulnerability in Bluetooth Stack Could Allow Remote Code Execution - Windows XP (x64) - CORRUPT PATCH
803005	MS08-030: Vulnerability in Bluetooth Stack Could Allow Remote Code Execution - Windows Vista Gold/SP1
803009	MS08-030: Vulnerability in Bluetooth Stack Could Allow Remote Code Execution - Windows Vista (x64)
803205	MS08-032: Cumulative Security Update of ActiveX Kill Bits - Windows XP Gold (x64)
803206	MS08-032: Cumulative Security Update of ActiveX Kill Bits - Windows XP Gold (x64) - CORRUPT PATCH

803211	MS08-032: Cumulative Security Update of ActiveX Kill Bits - Windows Vista Gold/SP1
803213	MS08-032: Cumulative Security Update of ActiveX Kill Bits - Windows Vista (x64)
803505	MS08-035: Vulnerability in Active Directory Could Allow Denial of Service - ADAM - Windows XP Gold (x64)
803506	MS08-035: Vulnerability in Active Directory Could Allow Denial of Service - ADAM - Windows XP Gold (x64) - CORRUPT PATCH
803603	MS08-036: Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service - Windows XP (x64)
803604	MS08-036: Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service - Windows XP (x64) - CORRUPT PATCH
803609	MS08-036: Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service - Windows Vista Gold/SP1
803611	MS08-036: Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service - Windows Vista (x64)
803705	MS08-037: Vulnerabilities in DNS Could Allow Spoofing - DNS Client - Windows XP Gold (x64)
803706	MS08-037: Vulnerabilities in DNS Could Allow Spoofing - DNS Client - Windows XP Gold (x64) - CORRUPT PATCH
804113	MS08-041: Vulnerability in the ActiveX Control for the Snapshot Viewer for Microsoft Access Could Allow Remote Code Execution - Office XP SP3 (Administrative Installation)
804601	MS08-046: Vulnerability in Microsoft Windows Image Color Management System Could Allow Remote Code Execution - Windows XP Gold/SP2 (x64)
804602	MS08-046: Vulnerability in Microsoft Windows Image Color Management System Could Allow Remote Code Execution - Windows XP Gold/SP2 (x64) - CORRUPT PATCH
804701	MS08-047: Vulnerability in IPsec Policy Processing Could Allow Information Disclosure - Windows Vista Gold/SP1
804703	MS08-047: Vulnerability in IPsec Policy Processing Could Allow Information Disclosure - Windows Vista Gold/SP1 (x64)
804809	MS08-048: Security Update for Outlook Express and Windows Mail - OE 6 - Windows XP Gold/SP2 (x64)
804810	MS08-048: Security Update for Outlook Express and Windows Mail - OE 6 - Windows XP Gold/SP2 (x64) - CORRUPT PATCH
804811	MS08-048: Security Update for Outlook Express and Windows Mail - OE 6 - Windows Server 2003 SP1/SP2
804812	MS08-048: Security Update for Outlook Express and Windows Mail - OE 6 - Windows Server 2003 SP1/SP2 - CORRUPT PATCH
804813	MS08-048: Security Update for Outlook Express and Windows Mail - OE 6 - Windows Server 2003 Gold/SP2 (x64)

804814	MS08-048: Security Update for Outlook Express and Windows Mail - OE 6 - Windows Server 2003 Gold/SP2 (x64) - CORRUPT PATCH
804815	MS08-048: Security Update for Outlook Express and Windows Mail - WM - Windows Vista Gold
804817	MS08-048: Security Update for Outlook Express and Windows Mail - WM - Windows Vista Gold (x64)
804905	MS08-049: Vulnerabilities in Event System Could Allow Remote Code Execution - Windows XP Gold/SP2 (x64)
804906	MS08-049: Vulnerabilities in Event System Could Allow Remote Code Execution - Windows XP Gold/SP2 (x64) - CORRUPT PATCH
804911	MS08-049: Vulnerabilities in Event System Could Allow Remote Code Execution - Windows Vista Gold/SP1
804913	MS08-049: Vulnerabilities in Event System Could Allow Remote Code Execution - Windows Vista Gold/SP1 (x64)
805003	MS08-050: Vulnerability in Windows Messenger Could Allow Information Disclosure - Windows Messenger 4.7 - Windows XP Gold/SP2 (x64)
805004	MS08-050: Vulnerability in Windows Messenger Could Allow Information Disclosure - Windows Messenger 4.7 - Windows XP Gold/SP2 (x64) - CORRUPT PATCH
805219	MS08-052: Vulnerabilities in GDI+ Could Allow Remote Code Execution - .NET Framework 1.0 SP3 - Windows 2000 SP4
805222	MS08-052: Vulnerabilities in GDI+ Could Allow Remote Code Execution - .NET Framework 1.0 SP3 - Windows 2000 SP4 - CORRUPT PATCH
805223	MS08-052: Vulnerabilities in GDI+ Could Allow Remote Code Execution - .NET Framework 2.0 - Windows 2000 SP4
805225	MS08-052: Vulnerabilities in GDI+ Could Allow Remote Code Execution - .NET Framework 2.0 SP1 - Windows 2000 SP4
805234	MS08-052: Vulnerabilities in GDI+ Could Allow Remote Code Execution - .NET Framework 2.0 - Windows 2000 SP4 - CORRUPT PATCH
805248	MS08-052: Vulnerabilities in GDI+ Could Allow Remote Code Execution - .NET Framework 2.0 SP1 - Windows 2000 SP4 - CORRUPT PATCH
805249	MS08-052: Vulnerabilities in GDI+ Could Allow Remote Code Execution - Visual FoxPro 9.0 SP2 - Windows 2000 SP4
805253	MS08-052: Vulnerabilities in GDI+ Could Allow Remote Code Execution - Forefront Client Security 1.0 - Windows 2000 SP4
805259	MS08-052: Vulnerabilities in GDI+ Could Allow Remote Code Execution - Windows XP Gold (x64) (v2
805260	MS08-052: Vulnerabilities in GDI+ Could Allow Remote Code Execution - Windows XP Gold(x64) (v2
805305	MS08-053: Vulnerability in Windows Media Encoder 9 (32-bit) Could Allow Remote Code Execution - Windows XP Gold (x64)

805306	MS08-053: Vulnerability in Windows Media Encoder 9 (32-bit) Could Allow Remote Code Execution - Windows XP Gold (x64) - CORRUPT PATCH
805307	MS08-053: Vulnerability in Windows Media Encoder 9 (64-bit) Could Allow Remote Code Execution - Windows XP Gold (x64)
805308	MS08-053: Vulnerability in Windows Media Encoder 9 (64-bit) Could Allow Remote Code Execution - Windows XP Gold (x64) - CORRUPT PATCH
805403	MS08-054: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Windows Media Player 11 - Windows XP Gold/SP2 (x64)
805404	MS08-054: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Windows Media Player 11 - Windows XP Gold/SP2 (x64) - CORRUPT PATCH
805405	MS08-054: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Windows Vista Gold/SP1
805407	MS08-054: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Windows Vista Gold/SP1 (x64)
805501	MS08-055: Vulnerability in Microsoft Office Could Allow Remote Code Execution - Office XP SP3 (Local/Network Installation)
805503	MS08-055: Vulnerability in Microsoft Office Could Allow Remote Code Execution - Office XP SP3 (Administrative Installation)
805601	MS08-056: Vulnerability in Microsoft Office Could Allow Information Disclosure - Office XP SP3 (Local/Network Installation)
805603	MS08-056: Vulnerability in Microsoft Office Could Allow Information Disclosure - Office XP SP3 (Administrative Installation)
806201	MS08-062: Vulnerability in Windows Internet Printing Service Could Allow Remote Code Execution - Windows 2000 SP4
806202	MS08-062: Vulnerability in Windows Internet Printing Service Could Allow Remote Code Execution - Windows 2000 SP4 - CORRUPT PATCH
806203	MS08-062: Vulnerability in Windows Internet Printing Service Could Allow Remote Code Execution - Windows XP SP2/SP3
806204	MS08-062: Vulnerability in Windows Internet Printing Service Could Allow Remote Code Execution - Windows XP SP2/SP3 - CORRUPT PATCH
806205	MS08-062: Vulnerability in Windows Internet Printing Service Could Allow Remote Code Execution - Windows XP Gold/SP2 (x64)
806206	MS08-062: Vulnerability in Windows Internet Printing Service Could Allow Remote Code Execution - Windows XP Gold/SP2 (x64) - CORRUPT PATCH
806211	MS08-062: Vulnerability in Windows Internet Printing Service Could Allow Remote Code Execution - Windows Vista Gold/SP1

806213	MS08-062: Vulnerability in Windows Internet Printing Service Could Allow Remote Code Execution - Windows Vista Gold/SP1 (x64)
806601	MS08-066: Vulnerability in the Microsoft Ancillary Function Driver Could Allow Elevation of Privilege - Windows XP SP2
806602	MS08-066: Vulnerability in the Microsoft Ancillary Function Driver Could Allow Elevation of Privilege - Windows XP SP2 - CORRUPT PATCH
806603	MS08-066: Vulnerability in the Microsoft Ancillary Function Driver Could Allow Elevation of Privilege - Windows XP Gold (x64)
806604	MS08-066: Vulnerability in the Microsoft Ancillary Function Driver Could Allow Elevation of Privilege - Windows XP Gold (x64) - CORRUPT PATCH
806701	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution - Windows 2000 SP4
806702	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution - Windows 2000 SP4 - CORRUPT PATCH
806703	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution - Windows XP SP2
806704	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution - Windows XP SP2 - CORRUPT PATCH
806705	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution - Windows XP Gold (x64)
806706	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution - Windows XP Gold (x64) - CORRUPT PATCH
806711	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution - Windows Vista Gold/SP1
806713	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution - Windows Vista Gold/SP1 (x64)
806801	MS08-068: Vulnerability in SMB Could Allow Remote Code Execution - Windows 2000 SP4
806802	MS08-068: Vulnerability in SMB Could Allow Remote Code Execution - Windows 2000 SP4 - CORRUPT PATCH
806805	MS08-068: Vulnerability in SMB Could Allow Remote Code Execution - Windows XP Gold (x64)
806806	MS08-068: Vulnerability in SMB Could Allow Remote Code Execution - Windows XP Gold (x64) - CORRUPT PATCH
806901	MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 3.0 - Windows 2000 SP4
806902	MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 3.0 - Windows 2000 SP4 - CORRUPT PATCH
806903	MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 4.0 - Windows 2000/XP/Vista/7

806904	MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 4.0 - Windows 2000/XP/Vista/7 - CORRUPT PATCH
806905	MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 6.0 - Windows 2000/XP
806907	MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 3.0 - Windows XP SP2
806908	MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 3.0 - Windows XP SP2 - CORRUPT PATCH
806911	MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 3.0 - Windows XP Gold(x64)
806912	MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 3.0 - Windows XP Gold(x64) - CORRUPT PATCH
806917	MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 3.0 - Windows Vista Gold
806919	MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 6.0 - Windows Vista Gold/SP1
806921	MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 3.0 - Windows Vista Gold(x64)
806923	MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 6.0 - Windows Vista Gold/SP1(x64)
806935	MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 5.0 - Office 2007/Office Compatibility Pack 2007/Expression Web
807021	MS08-070: Vulnerabilities in Visual Basic 6.0 Runtime Extended Files (ActiveX Controls) Could Allow Remote Code Execution - Visual FoxPro 8.0 SP1
807022	MS08-070: Vulnerabilities in Visual Basic 6.0 Runtime Extended Files (ActiveX Controls) Could Allow Remote Code Execution - Visual FoxPro 8.0 SP1 - CORRUPT PATCH
807026	MS08-070: Vulnerabilities in Visual Basic 6.0 Runtime Extended Files (ActiveX Controls) Could Allow Remote Code Execution - Visual FoxPro 9.0 SP1
807027	MS08-070: Vulnerabilities in Visual Basic 6.0 Runtime Extended Files (ActiveX Controls) Could Allow Remote Code Execution - Visual FoxPro 9.0 SP1 - CORRUPT PATCH

807031	MS08-070: Vulnerabilities in Visual Basic 6.0 Runtime Extended Files (ActiveX Controls) Could Allow Remote Code Execution - Visual FoxPro 9.0 SP2
807032	MS08-070: Vulnerabilities in Visual Basic 6.0 Runtime Extended Files (ActiveX Controls) Could Allow Remote Code Execution - Visual FoxPro 9.0 SP2 - CORRUPT PATCH
807105	MS08-071: Vulnerabilities in GDI Could Allow Remote Code Execution - Windows XP Gold (x64)
807106	MS08-071: Vulnerabilities in GDI Could Allow Remote Code Execution - Windows XP Gold (x64) - CORRUPT PATCH
807111	MS08-071: Vulnerabilities in GDI Could Allow Remote Code Execution - Windows Vista Gold/SP1
807113	MS08-071: Vulnerabilities in GDI Could Allow Remote Code Execution - Windows Vista Gold/SP1 (x64)
807501	MS08-075: Vulnerabilities in Windows Search Could Allow Remote Code Execution - Windows Search - Windows Vista
807503	MS08-075: Vulnerabilities in Windows Search Could Allow Remote Code Execution - Windows Explorer - Windows Vista
807505	MS08-075: Vulnerabilities in Windows Search Could Allow Remote Code Execution - Windows Search - Windows Vista (x64)
807507	MS08-075: Vulnerabilities in Windows Search Could Allow Remote Code Execution - Windows Explorer - Windows Vista (x64)
807511	MS08-075: Vulnerabilities in Windows Search Could Allow Remote Code Execution - Windows Explorer - Windows Server 2008
807515	MS08-075: Vulnerabilities in Windows Search Could Allow Remote Code Execution - Windows Explorer - Windows Server 2008 (x64)
807605	MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution - Windows Media Player 6.4 - Windows XP Gold (x64)
807606	MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution - Windows Media Player 6.4 - Windows XP Gold (x64) - CORRUPT PATCH
807617	MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 - Windows XP Gold/SP2 (x64)
807618	MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 - Windows XP Gold/SP2 (x64) - CORRUPT PATCH
807619	MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 x64 Edition - Windows XP/2003 (x64)
807620	MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 x64 Edition - Windows XP/2003 (x64) - CORRUPT PATCH

807621	MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution - Windows Media Format Runtime 11 Edition - Windows XP Gold/SP2 (x64)
807622	MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution - Windows Media Format Runtime 11 Edition - Windows XP Gold/SP2 (x64) - CORRUPT PATCH
807627	MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution - Windows Media Format Runtime 11 - Windows Vista Gold/SP1
807629	MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution - Windows Media Format Runtime 11 - Windows Vista Gold/SP1 (x64)
900105	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution - Windows XP Gold (x64)
900106	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution - Windows XP Gold(x64) - CORRUPT PATCH
900705	MS09-007: Vulnerability in SChannel Could Allow Spoofing - Windows XP Gold/SP2 (x64)
900706	MS09-007: Vulnerability in SChannel Could Allow Spoofing - Windows XP Gold/SP2 (x64) - CORRUPT PATCH
900711	MS09-007: Vulnerability in SChannel Could Allow Spoofing - Windows Vista Gold/SP1
900713	MS09-007: Vulnerability in SChannel Could Allow Spoofing - Windows Vista Gold/SP1 (x64)
901005	MS09-010: Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution - Windows XP/2003 (x64)
901014	MS09-010: Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution - Windows XP/2003 (x64) - CORRUPT PATCH
901107	MS09-011: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution - DirectX 9.0 - Windows XP Gold (x64)
901108	MS09-011: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution - DirectX 9.0 - Windows XP Gold (x64) - CORRUPT PATCH
901207	MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege - MSDTC Transaction Facility - Windows XP Gold/SP2 (x64)
901208	MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege - MSDTC Transaction Facility - Windows XP Gold/SP2 (x64) - CORRUPT PATCH
901209	MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege - Windows Service Isolation - Windows XP Gold/SP2 (x64)
901210	MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege - Windows Service Isolation - Windows XP Gold/SP2 (x64) - CORRUPT PATCH

901219	MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege - MSDTC Transaction Facility - Windows Vista Gold/SP1
901221	MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege - Windows Service Isolation - Windows Vista Gold/SP1
901223	MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege - MSDTC Transaction Facility - Windows Vista Gold/SP1 (x64)
901225	MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege - Windows Service Isolation - Windows Vista Gold/SP1 (x64)
901305	MS09-013: Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution - Windows XP Gold/SP2 (x64)
901311	MS09-013: Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution - Windows Vista Gold/SP1
901313	MS09-013: Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution - Windows Vista Gold/SP1 (x64)
901407	MS09-014: Cumulative Security Update for Internet Explorer - IE 6 - Windows XP Gold (x64)
901408	MS09-014: Cumulative Security Update for Internet Explorer - IE 6 - Windows XP Gold (x64) - CORRUPT PATCH
901409	MS09-014: Cumulative Security Update for Internet Explorer - IE 6 - Windows Server 2003 SP1
901410	MS09-014: Cumulative Security Update for Internet Explorer - IE 6 - Windows Server 2003 SP1 - CORRUPT PATCH
901411	MS09-014: Cumulative Security Update for Internet Explorer - IE 6 - Windows Server 2003 Gold (x64)
901412	MS09-014: Cumulative Security Update for Internet Explorer - IE 6 - Windows Server 2003 Gold (x64) - CORRUPT PATCH
901415	MS09-014: Cumulative Security Update for Internet Explorer - IE 7 - Windows XP Gold (x64)
901416	MS09-014: Cumulative Security Update for Internet Explorer - IE 7 - Windows XP Gold (x64) - CORRUPT PATCH
901417	MS09-014: Cumulative Security Update for Internet Explorer - IE 7 - Windows Server 2003 SP1
901418	MS09-014: Cumulative Security Update for Internet Explorer - IE 7 - Windows Server 2003 SP1 - CORRUPT PATCH
901419	MS09-014: Cumulative Security Update for Internet Explorer - IE 7 - Windows Server 2003 Gold (x64)
901420	MS09-014: Cumulative Security Update for Internet Explorer - IE 7 - Windows Server 2003 Gold (x64) - CORRUPT PATCH
901505	MS09-015: Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege - Windows XP Gold/SP2 (x64)
901506	MS09-015: Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege - Windows XP Gold/SP2 (x64) - CORRUPT PATCH

901511	MS09-015: Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege - Windows Vista Gold/SP1
901513	MS09-015: Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege - Windows Vista Gold/SP1 (x64)
902005	MS09-020: Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege - IIS 6.0 - Windows XP SP2 (x64)
902006	MS09-020: Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege - IIS 6.0 - Windows XP SP2 (x64) - CORRUPT PATCH
902211	MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution - Windows Vista Gold/SP1
902213	MS09-022: Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution - Windows Vista Gold/SP1 (x64)
902303	MS09-023: Vulnerability in Windows Search Could Allow Information Disclosure - Windows Search 4.0 - Windows XP SP2 (x64)
902304	MS09-023: Vulnerability in Windows Search Could Allow Information Disclosure - Windows Search 4.0 - Windows XP SP2 (x64) - CORRUPT PATCH
902408	MS09-024: Vulnerability in Microsoft Works Converters Could Allow Remote Code Execution - Office XP SP3 (Administrative Installation)
902611	MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege - Windows Vista Gold/SP1
902613	MS09-026: Vulnerability in RPC Could Allow Elevation of Privilege - Windows Vista Gold/SP1 (x64)
903602	MS09-036: Vulnerability in ASP.NET in Microsoft Windows Could Allow Denial of Service - .NET Framework 2.0 SP1 / 3.5 - Windows Vista Gold (x64)
903603	MS09-036: Vulnerability in ASP.NET in Microsoft Windows Could Allow Denial of Service - .NET Framework 2.0 SP2 / 3.5 SP1 - Windows Vista Gold (x64)
903611	MS09-036: Vulnerability in ASP.NET in Microsoft Windows Could Allow Denial of Service - .NET Framework 2.0 SP1/3.5 - Windows Vista Gold
903613	MS09-036: Vulnerability in ASP.NET in Microsoft Windows Could Allow Denial of Service - .NET Framework 2.0 SP2/3.5 SP1 - Windows Vista Gold
903727	MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution - Windows Media Player 10 - Windows XP SP2 (x64)
903728	MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution - Windows Media Player 10 - Windows XP SP2 (x64) - CORRUPT PATCH
903729	MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution - Windows Media Player 11- Windows XP SP2 (x64)

903731	MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution - Windows ATL Component - Windows XP SP2 (x64)
903732	MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution - Windows ATL Component - Windows XP SP2 (x64) - CORRUPT PATCH
903733	MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution - DHTML Editing Component ActiveX Control - Windows XP SP2 (x64)
903734	MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution - DHTML Editing Component ActiveX Control - Windows XP SP2 (x64) - CORRUPT PATCH
903735	MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution - MSWebDVD ActiveX Control - Windows XP SP2 (x64)
903736	MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution - MSWebDVD ActiveX Control - Windows XP SP2 (x64) - CORRUPT PATCH
903757	MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution - Windows Media Player 11 - Windows Vista Gold/SP1/SP2
903759	MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution - Windows ATL Component - Windows Vista Gold/SP1/SP2
903761	MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution - Windows Media Player 11 - Windows Vista Gold/SP1/SP2 (x64)
903763	MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution - Windows ATL Component - Windows Vista Gold/SP1/SP2 (x64)
903773	MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution - HtmlInput Object ActiveX Control - Windows Vista Gold/SP1/SP2
903775	MS09-037: Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution - HtmlInput Object ActiveX Control - Windows Vista Gold/SP1/SP2 (x64)
904005	MS09-040: Vulnerability in Message Queuing Could Allow Elevation of Privilege - Windows XP SP2 (x64)
904006	MS09-040: Vulnerability in Message Queuing Could Allow Elevation of Privilege - Windows XP SP2 (x64) - CORRUPT PATCH
904011	MS09-040: Vulnerability in Message Queuing Could Allow Elevation of Privilege - Windows Vista Gold
904013	MS09-040: Vulnerability in Message Queuing Could Allow Elevation of Privilege - Windows Vista Gold (x64)

904103	MS09-041: Vulnerability in Workstation Service Could Allow Elevation of Privilege - Windows XP SP2 (x64)
904104	MS09-041: Vulnerability in Workstation Service Could Allow Elevation of Privilege - Windows XP SP2 (x64) - CORRUPT PATCH
904109	MS09-041: Vulnerability in Workstation Service Could Allow Elevation of Privilege - Windows Vista Gold/SP1/SP2
904111	MS09-041: Vulnerability in Workstation Service Could Allow Elevation of Privilege - Windows Vista Gold/SP1/SP2 (x64)
904205	MS09-042: Vulnerability in Telnet Could Allow Remote Code Execution - Windows XP SP2 (x64)
904206	MS09-042: Vulnerability in Telnet Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
904211	MS09-042: Vulnerability in Telnet Could Allow Remote Code Execution - Windows Vista Gold/SP1/SP2
904213	MS09-042: Vulnerability in Telnet Could Allow Remote Code Execution - Windows Vista Gold/SP1/SP2 (x64)
904303	MS09-043: Vulnerabilities in Microsoft Office Web Components Could Allow Remote Code Execution - Office XP SP3 (Administrative Installation)
904411	MS09-044: Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution - RDP 5.2 - Windows XP SP2 (x64)
904412	MS09-044: Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution - RDP 5.2 - Windows XP SP2 (x64) - CORRUPT PATCH
904413	MS09-044: Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution - RDP 6.0/6.1 - Windows XP SP2 (x64)
904414	MS09-044: Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution - RDP 6.0/6.1 - Windows XP SP2 (x64) - CORRUPT PATCH
904423	MS09-044: Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution - RDP 6.0/6.1 - Windows Vista Gold/SP1
904425	MS09-044: Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution - RDP 6.0/6.1 - Windows Vista Gold/SP1 (x64)
904527	MS09-045: Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution - JScript 5.7 - Windows Vista Gold
904529	MS09-045: Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution - JScript 5.7 - Windows Vista Gold (x64)
904531	MS09-045: Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution - JScript 5.8 - Windows Vista Gold (x64)
904533	MS09-045: Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution - JScript 5.8 - Windows Vista Gold
904605	MS09-046: Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution - Windows XP SP2 (x64)

904606	MS09-046: Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
904717	MS09-047: Vulnerabilities in Windows Media Format Could Allow Remote Code Execution - Windows Media Format Runtime 11 - Windows Vista Gold/SP1/SP2
904719	MS09-047: Vulnerabilities in Windows Media Format Could Allow Remote Code Execution - Windows Media Format Runtime 11 - Windows Vista Gold/SP1/SP2 (x64)
904733	MS09-047: Vulnerabilities in Windows Media Format Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 (x64) - Windows XP SP2 (x64)
904734	MS09-047: Vulnerabilities in Windows Media Format Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 (x64) - Windows XP SP2 (x64) - CORRUPT PATCH
904805	MS09-048: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution - Windows Vista Gold/SP1/SP2
904807	MS09-048: Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution - Windows Vista Gold/SP1/SP2 (x64)
904901	MS09-049: Vulnerability in Wireless LAN AutoConfig Service Could Allow Remote Code Execution - Windows Vista Gold/SP1/SP2
904903	MS09-049: Vulnerability in Wireless LAN AutoConfig Service Could Allow Remote Code Execution - Windows Vista Gold/SP1/SP2 (x64)
905101	MS09-051: Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution - DirectShow WMA Voice Codec - Windows 2000 SP4 / 2003 SP2 / XP SP2/SP3
905102	MS09-051: Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution - DirectShow WMA Voice Codec - Windows 2000 SP4 / 2003 SP2 / XP SP2/SP3 - CORRUPT PATCH
905115	MS09-051: Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution - Windows Media Audio Voice Decoder - Windows XP SP2 (x64)
905116	MS09-051: Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution - Windows Media Audio Voice Decoder - Windows XP SP2 (x64) - CORRUPT PATCH
905119	MS09-051: Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution - Windows Media Audio Voice Decoder in Windows Media Format SDK 11 - Windows XP SP2 (x64)
905120	MS09-051: Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution - Windows Media Audio Voice Decoder in Windows Media Format SDK 11 - Windows XP SP2 (x64) - CORRUPT PATCH

905129	MS09-051: Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution - Windows Media Audio Voice Decoder - Windows Vista Gold/SP1/SP2
905131	MS09-051: Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution - Windows Media Audio Voice Decoder - Windows Vista Gold/SP1/SP2 (x64)
905137	MS09-051: Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution - Audio Compression Manager - Windows XP SP2 (x64)
905138	MS09-051: Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution - Audio Compression Manager - Windows XP SP2 (x64) - CORRUPT PATCH
905143	MS09-051: Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution - DirectShow WMA Voice Codec - Windows XP SP2 (x64)
905144	MS09-051: Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution - DirectShow WMA Voice Codec - Windows XP SP2 (x64) - CORRUPT PATCH
905205	MS09-052: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Microsoft Windows Media Player 6.4 - Windows XP SP2 (x64)
905206	MS09-052: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Microsoft Windows Media Player 6.4 - Windows XP SP2 (x64) - CORRUPT PATCH
905305	MS09-053: Vulnerabilities in FTP Service for Internet Information Services Could Allow Remote Code Execution - IIS 5.1 - Windows XP SP2 (x64)
905306	MS09-053: Vulnerabilities in FTP Service for Internet Information Services Could Allow Remote Code Execution - IIS 5.1 - Windows XP SP2 (x64) - CORRUPT PATCH
905311	MS09-053: Vulnerabilities in FTP Service for Internet Information Services Could Allow Remote Code Execution - IIS 7.0 - Windows Vista Gold/SP1/SP2
905313	MS09-053: Vulnerabilities in FTP Service for Internet Information Services Could Allow Remote Code Execution - IIS 7.0 - Windows Vista Gold/SP1/SP2 (x64)
905605	MS09-056: Vulnerabilities in Windows CryptoAPI Could Allow Spoofing - Windows XP Pro SP2 (x64)
905606	MS09-056: Vulnerabilities in Windows CryptoAPI Could Allow Spoofing - Windows XP Pro SP2 (x64) - CORRUPT PATCH
905611	MS09-056: Vulnerabilities in Windows CryptoAPI Could Allow Spoofing - Windows Vista Gold/SP1/SP2
905613	MS09-056: Vulnerabilities in Windows CryptoAPI Could Allow Spoofing - Windows Vista Gold/SP1/SP2 (x64)

905619	MS09-056: Vulnerabilities in Windows CryptoAPI Could Allow Spoofing - Windows 7
905621	MS09-056: Vulnerabilities in Windows CryptoAPI Could Allow Spoofing - Windows 7 (x64)
905705	MS09-057: Vulnerability in Indexing Service Could Allow Remote Code Execution - Windows XP SP2 (x64)
905706	MS09-057: Vulnerability in Indexing Service Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
905903	MS09-059: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service - Windows XP SP2 (x64)
905904	MS09-059: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service - Windows XP SP2 (x64) - CORRUPT PATCH
905909	MS09-059: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service - Windows Vista Gold/SP1/SP2
905911	MS09-059: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service - Windows Vista Gold/SP1/SP2 (x64)
905917	MS09-059: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service - Windows 7
905919	MS09-059: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service - Windows 7 (x64)
906103	MS09-061: Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow Remote Code Execution - .NET Framework 2.0 SP1/3.5 - Windows 2000 SP4 / XP SP2
906104	MS09-061: Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow Remote Code Execution - .NET Framework 2.0 SP1/3.5 - Windows 2000 SP4 / XP SP2- CORRUPT PATCH
906105	MS09-061: Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow Remote Code Execution - .NET Framework 2.0 SP2 / 3.5 SP1 - Windows 2000 SP4 / XP SP2
906106	MS09-061: Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow Remote Code Execution - .NET Framework 2.0 SP2 / 3.5 SP1 - Windows 2000 SP4 / XP SP2 - CORRUPT PATCH
906113	MS09-061: Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow Remote Code Execution - .NET Framework 2.0 - Windows Vista Gold (x64)
906115	MS09-061: Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow Remote Code Execution - .NET Framework 2.0 SP2/3.5 SP1 - Windows Vista Gold (x64)
906131	MS09-061: Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow Remote Code Execution - .NET Framework 2.0 - Windows Vista Gold

906133	MS09-061: Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow Remote Code Execution - .NET Framework 2.0 SP2/3.5 SP1 - Windows Vista Gold
906209	MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution - Windows Vista Gold
906211	MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution - Windows Vista Gold (x64)
906219	MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution - .NET Framework 1.1 SP1 - Windows 2000 SP4
906221	MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution - .NET Framework 2.0 SP1 - Windows 2000 SP4
906222	MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution - .NET Framework 1.1 SP1 - Windows 2000 SP4 - CORRUPT PATCH
906223	MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution - .NET Framework 2.0 SP2 - Windows 2000 SP4
906224	MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution - .NET Framework 2.0 SP1 - Windows 2000 SP4 - CORRUPT PATCH
906225	MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution - .NET Framework 2.0 SP2 - Windows 2000 SP4 - CORRUPT PATCH
906301	MS09-063: Vulnerability in Web Services on Devices API Could Allow Remote Code Execution - Windows Vista Gold/SP1/SP2
906303	MS09-063: Vulnerability in Web Services on Devices API Could Allow Remote Code Execution - Windows Vista Gold/SP1/SP2 (x64)
906511	MS09-065: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - Windows Vista Gold/SP1
906513	MS09-065: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - Windows Vista Gold/SP1 (x64)
906905	MS09-069: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service - Windows XP SP2 (x64)
906906	MS09-069: Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service - Windows XP SP2 (x64) - CORRUPT PATCH
907105	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution - Windows XP SP2 (x64)
907106	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
907111	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution - Windows Vista Gold/SP1/SP2
907113	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution - Windows Vista Gold/SP1/SP2 (x64)
907305	MS09-073: Vulnerability in WordPad and Office Text Converters Could Allow Remote Code Execution - Windows XP SP2 (x64)

907308	MS09-073: Vulnerability in WordPad and Office Text Converters Could Allow Remote Code Execution - Office XP SP3 (Administrative Installation)
907310	MS09-073: Vulnerability in WordPad and Office Text Converters Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1000105	MS10-001: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution - Windows XP SP2 (x64)
1000106	MS10-001: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1000111	MS10-001: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution - Windows Vista Gold/SP1/SP2
1000113	MS10-001: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution - Windows Vista Gold/SP1/SP2 (x64)
1000119	MS10-001: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution - Windows 7
1000121	MS10-001: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution - Windows 7 (x64)
1000505	MS10-005: Vulnerability in Microsoft Paint Could Allow Remote Code Execution - Windows XP SP2 (x64)
1000506	MS10-005: Vulnerability in Microsoft Paint Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1000705	MS10-007: Vulnerability in Windows Shell Handler Could Allow Remote Code Execution - Windows XP SP2 (x64)
1000706	MS10-007: Vulnerability in Windows Shell Handler Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1000811	MS10-008: Cumulative Security Update of ActiveX Kill Bits - Windows Vista Gold/SP1
1000813	MS10-008: Cumulative Security Update of ActiveX Kill Bits - Windows Vista SP1/SP2 (x64)
1001211	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution - Windows Vista Gold
1001213	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution - Windows Vista Gold (x64)
1001311	MS10-013: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution - AVI Filter - Windows XP SP2 (x64)
1001312	MS10-013: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution - AVI Filter - Windows XP SP2 (x64) - CORRUPT PATCH
1001313	MS10-013: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution - Quartz - Windows XP SP2 (x64)
1001314	MS10-013: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution - Quartz - Windows XP SP2 (x64) - CORRUPT PATCH

1001323	MS10-013: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution - Quartz - Windows Vista Gold/SP1/SP2
1001325	MS10-013: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution - Quartz - Windows Vista Gold/SP1/SP2 (x64)
1001331	MS10-013: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution - Quartz - Windows 7
1001333	MS10-013: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution - Quartz - Windows 7 (x64)
1001519	MS10-015: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege - Windows 7
1001605	MS10-016: Vulnerability in Windows Movie Maker Could Allow Remote Code Execution - Movie Maker 6.0 - Windows Vista Gold
1001911	MS10-019: Vulnerabilities in Windows Could Allow Remote Code Execution - Cabinet File Viewer Shell Extension 6.0 - Windows XP SP2 (x64)
1001912	MS10-019: Vulnerabilities in Windows Could Allow Remote Code Execution - Cabinet File Viewer Shell Extension 6.0 - Windows XP SP2 (x64) - CORRUPT PATCH
1001923	MS10-019: Vulnerabilities in Windows Could Allow Remote Code Execution - Cabinet File Viewer Shell Extension 6.0 - Windows Vista Gold/SP1/SP2
1001927	MS10-019: Vulnerabilities in Windows Could Allow Remote Code Execution - Cabinet File Viewer Shell Extension 6.0 - Windows Vista Gold/SP1/SP2 (x64)
1001945	MS10-019: Vulnerabilities in Windows Could Allow Remote Code Execution - Cabinet File Viewer Shell Extension 6.1 - Windows 7 (x64)
1001947	MS10-019: Vulnerabilities in Windows Could Allow Remote Code Execution - Cabinet File Viewer Shell Extension 6.1 - Windows 7
1002009	MS10-020: Vulnerabilities in SMB Client Could Allow Remote Code Execution - Windows Vista Gold
1002011	MS10-020: Vulnerabilities in SMB Client Could Allow Remote Code Execution - Windows Vista Gold (x64)
1002112	MS10-021: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege - Windows Vista Gold
1002113	MS10-021: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege - Windows Vista Gold (x64)
1002225	MS10-022: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution - VBScript 5.7 - Windows Vista Gold
1002227	MS10-022: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution - VBScript 5.7 - Windows Vista Gold (x64)
1002239	MS10-022: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution - VBScript 5.8 - Windows Vista Gold (x64)

1002245	MS10-022: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution - VBScript 5.8 - Windows Vista Gold
1002405	MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service - Windows XP SP2 (x64)
1002406	MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service - Windows XP SP2 (x64) - CORRUPT PATCH
1002605	MS10-026: Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution - MPEG Layer-3 codecs - Windows XP SP2 (x64)
1002606	MS10-026: Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution - MPEG Layer-3 codecs - Windows XP SP2 (x64) - CORRUPT PATCH
1002611	MS10-026: Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution - MPEG Layer-3 codecs - Windows Vista Gold/SP1/SP2
1002613	MS10-026: Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution - MPEG Layer-3 codecs - Windows Vista Gold/SP1/SP2 (x64)
1002903	MS10-029: Vulnerability in Windows ISATAP Component Could Allow Spoofing - Windows XP SP2 (x64)
1002904	MS10-029: Vulnerability in Windows ISATAP Component Could Allow Spoofing - Windows XP SP2 (x64) - CORRUPT PATCH
1002909	MS10-029: Vulnerability in Windows ISATAP Component Could Allow Spoofing - Windows Vista Gold/SP1/SP2
1002911	MS10-029: Vulnerability in Windows ISATAP Component Could Allow Spoofing - Windows Vista Gold/SP1/SP2 (x64)
1003007	MS10-030: Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution - OE 6 - Windows Live Mail - Windows XP SP2 (x64)
1003008	MS10-030: Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution - OE 6 - Windows Live Mail - Windows XP SP2 (x64) - CORRUPT PATCH
1003009	MS10-030: Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution - OE 6 - Windows Server 2003 SP2
1003010	MS10-030: Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution - OE 6 - Windows Server 2003 SP2 - CORRUPT PATCH
1003011	MS10-030: Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution - OE 6 - Windows Server 2003 SP2 (x64)
1003012	MS10-030: Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution - OE 6 - Windows Server 2003 SP2 (x64) - CORRUPT PATCH

1003019	MS10-030: Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution - Windows Mail - Windows Live Mail - Windows Server 2008 Gold (x64)
1003021	MS10-030: Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution - Windows Mail - Windows Live Mail - Windows 7
1003023	MS10-030: Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution - Windows Mail - Windows Live Mail - Windows 7 (x64)
1003025	MS10-030: Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution - Windows Mail - Windows Live Mail - Windows Server 2008 R2 (x64)
1003101	MS10-031: Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution - Office XP SP3 (Local/Network Installation)
1003103	MS10-031: Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution - Office XP SP3 (Administrative Installation)
1003319	MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 (32-bit) - Windows XP SP2 (x64)
1003320	MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 (32-bit) - Windows XP SP2 (x64) - CORRUPT PATCH
1003321	MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 (64-bit) - Windows XP/2003 (x64)
1003322	MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 (64-bit) - Windows XP/2003 (x64) - CORRUPT PATCH
1003323	MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution - Windows Media Format Runtime 11 - Windows XP SP2 (x64)
1003324	MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution - Windows Media Format Runtime 11 - Windows XP SP2 (x64) - CORRUPT PATCH
1003329	MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution - Asycfilt.dll (COM component) - Windows XP SP2 (x64)
1003330	MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution - Asycfilt.dll (COM component) - Windows XP SP2 (x64) - CORRUPT PATCH
1003343	MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution - Quartz.dll (DirectShow) - Windows Vista SP1

1003345	MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution - Asycfilt.dll (COM component) - Windows Vista SP1/SP2
1003349	MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution - Quartz.dll (DirectShow) - Windows Vista SP1 (x64)
1003351	MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution - Asycfilt.dll (COM component) - Windows Vista SP1/SP2 (x64)
1003367	MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution - Asycfilt.dll (COM component) - Windows 7
1003369	MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution - Asycfilt.dll (COM component) - Windows 7 (x64)
1003505	MS10-035: Cumulative Security Update for Internet Explorer - IE 6 - Windows XP SP2
1003506	MS10-035: Cumulative Security Update for Internet Explorer - IE 6 - Windows XP SP2 - CORRUPT PATCH
1003513	MS10-035: Cumulative Security Update for Internet Explorer - IE 7 - Windows XP SP2
1003514	MS10-035: Cumulative Security Update for Internet Explorer - IE 7 - Windows XP SP2 - CORRUPT PATCH
1003529	MS10-035: Cumulative Security Update for Internet Explorer - IE 8 - Windows XP SP2
1003530	MS10-035: Cumulative Security Update for Internet Explorer - IE 8 - Windows XP SP2 - CORRUPT PATCH
1004005	MS10-040: Vulnerability in Internet Information Services Could Allow Remote Code Execution - Internet Information Services 7.0 - Windows Vista SP1
1004007	MS10-040: Vulnerability in Internet Information Services Could Allow Remote Code Execution - Internet Information Services 7.0 - Windows Vista SP1 (x64)
1004013	MS10-040: Vulnerability in Internet Information Services Could Allow Remote Code Execution - Internet Information Services 7.5 - Windows 7
1004015	MS10-040: Vulnerability in Internet Information Services Could Allow Remote Code Execution - Internet Information Services 7.5 - Windows 7 (x64)
1004105	MS10-041: Vulnerability in Microsoft .NET Framework Could Allow Tampering - Microsoft .NET Framework 1.0 SP3 (Windows XP Media Center Edition / Tablet PC Edition)
1004106	MS10-041: Vulnerability in Microsoft .NET Framework Could Allow Tampering - Microsoft .NET Framework 1.0 SP3 (Windows XP Media Center Edition / Tablet PC Edition) - CORRUPT PATCH

1004107	MS10-041: Vulnerability in Microsoft .NET Framework Could Allow Tampering - Microsoft .NET Framework 3.5 - Windows XP/2003
1004111	MS10-041: Vulnerability in Microsoft .NET Framework Could Allow Tampering - Microsoft .NET Framework 2.0 SP1 / 3.5 - Windows Vista SP1 / Windows Server 2008 Gold
1004113	MS10-041: Vulnerability in Microsoft .NET Framework Could Allow Tampering - Microsoft .NET Framework 2.0 SP2 / 3.5 SP1 - Windows Vista SP1 / Windows Server 2008 Gold
1004141	MS10-041: Vulnerability in Microsoft .NET Framework Could Allow Tampering - .NET Framework 2.0 SP1 / 3.5 Gold - Windows XP/2003 (x64)
1004143	MS10-041: Vulnerability in Microsoft .NET Framework Could Allow Tampering - .NET Framework 2.0 SP1 / 3.5 Gold - Windows Vista/2008 (x64)
1004145	MS10-041: Vulnerability in Microsoft .NET Framework Could Allow Tampering - .NET Framework 2.0 SP2 / 3.5 SP1 - Windows Vista SP1 / Windows Server 2008 Gold (x64)
1004203	MS10-042: Vulnerability in Help and Support Center Could Allow Remote Code Execution - Windows XP SP2 (x64)
1004204	MS10-042: Vulnerability in Help and Support Center Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1004301	MS10-043: Vulnerability in Canonical Display Driver Could Allow Remote Code Execution - Windows 7 (x64)
1004503	MS10-045: Vulnerability in Microsoft Office Outlook Could Allow Remote Code Execution - Office XP SP3 (Administrative Installation)
1005003	MS10-050: Vulnerability in Windows Movie Maker Could Allow Remote Code Execution - Movie Maker 2.1 - Windows XP SP2 (x64)
1005004	MS10-050: Vulnerability in Windows Movie Maker Could Allow Remote Code Execution - Movie Maker 2.1 - Windows XP SP2 (x64) - CORRUPT PATCH
1005005	MS10-050: Vulnerability in Windows Movie Maker Could Allow Remote Code Execution - Movie Maker 6.0 - Windows Vista SP1/SP2
1005009	MS10-050: Vulnerability in Windows Movie Maker Could Allow Remote Code Execution - Movie Maker 6.0 - Windows Vista SP1/SP2 (x64)
1005203	MS10-052: Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution - Windows XP SP2 (x64)
1005204	MS10-052: Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1005503	MS10-055: Vulnerability in Cinepak Codec Could Allow Remote Code Execution - Windows XP SP2 (x64)
1005504	MS10-055: Vulnerability in Cinepak Codec Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1005505	MS10-055: Vulnerability in Cinepak Codec Could Allow Remote Code Execution - Windows Vista SP1/SP2

1005507	MS10-055: Vulnerability in Cinepak Codec Could Allow Remote Code Execution - Windows Vista SP1/SP2 (x64)
1005509	MS10-055: Vulnerability in Cinepak Codec Could Allow Remote Code Execution - Windows 7
1005511	MS10-055: Vulnerability in Cinepak Codec Could Allow Remote Code Execution - Windows 7 (x64)
1005801	MS10-058: Vulnerabilities in TCP/IP Could Allow Elevation of Privilege - Windows Vista SP1
1005803	MS10-058: Vulnerabilities in TCP/IP Could Allow Elevation of Privilege - Windows Vista SP1 (x64)
1005901	MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege - Windows Vista SP1/SP2
1005903	MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege - Windows Vista SP1/SP2 (x64)
1005909	MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege - Windows 7
1005911	MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege - Windows 7 (x64)
1006103	MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution - Windows XP SP2 (x64)
1006104	MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1006109	MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution - Windows Vista SP1/SP2
1006111	MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution - Windows Vista SP1/SP2 (x64)
1006117	MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution - Windows 7 Gold
1006119	MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution - Windows 7 Gold (x64)
1006203	MS10-062: Vulnerability in MPEG-4 Codec Could Allow Remote Code Execution - Windows XP SP2 (x64)
1006204	MS10-062: Vulnerability in MPEG-4 Codec Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1006209	MS10-062: Vulnerability in MPEG-4 Codec Could Allow Remote Code Execution - Windows Vista SP1/SP2
1006211	MS10-062: Vulnerability in MPEG-4 Codec Could Allow Remote Code Execution - Windows Vista SP1/SP2 (x64)
1006308	MS10-063: Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution - Office XP SP3 (Administrative Installation)
1006503	MS10-065: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution - ASP - Windows XP SP2 (x64)

1006504	MS10-065: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution - ASP - Windows XP SP2 (x64) - CORRUPT PATCH
1006509	MS10-065: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution - ASP - Windows Vista SP1/SP2
1006511	MS10-065: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution - ASP - Windows Vista SP1/SP2 (x64)
1006517	MS10-065: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution - ASP - Windows 7
1006519	MS10-065: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution - ASP - Windows 7 (x64)
1006523	MS10-065: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution - FastCGI - Windows 7
1006525	MS10-065: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution - FastCGI - Windows 7 (x64)
1007010	MS10-070: Vulnerability in ASP.NET Could Allow Information Disclosure - Microsoft .NET Framework 2.0 SP1 / 3.5 - Windows XP SP2 / Windows Server 2003 SP2 (x64)
1007011	MS10-070: Vulnerability in ASP.NET Could Allow Information Disclosure - Microsoft .NET Framework 2.0 SP1 / 3.5 - Windows XP SP3 / Windows Server 2003 SP2
1007012	MS10-070: Vulnerability in ASP.NET Could Allow Information Disclosure - Microsoft .NET Framework 2.0 SP1 / 3.5 - Windows XP SP3 / Windows Server 2003 SP2 - CORRUPT PATCH
1007014	MS10-070: Vulnerability in ASP.NET Could Allow Information Disclosure - Microsoft .NET Framework 2.0 SP1 / 3.5 - Windows XP SP2 / Windows Server 2003 SP2 (x64) - CORRUPT PATCH
1007023	MS10-070: Vulnerability in ASP.NET Could Allow Information Disclosure - Microsoft .NET Framework 2.0 SP1 / 3.5 - Windows Vista SP1 / Windows Server 2008 Gold
1007025	MS10-070: Vulnerability in ASP.NET Could Allow Information Disclosure - Microsoft .NET Framework 2.0 SP1 / 3.5 - Windows Vista SP1 / Windows Server 2008 Gold (x64)
1007027	MS10-070: Vulnerability in ASP.NET Could Allow Information Disclosure - Microsoft .NET Framework 2.0 SP2 / 3.5 SP1 - Windows Vista SP1 / Windows Server 2008 Gold
1007035	MS10-070: Vulnerability in ASP.NET Could Allow Information Disclosure - Microsoft .NET Framework 3.5 - Windows XP SP3 / Windows Server 2003 SP2 / Windows Vista SP2 / Windows Server 2008 SP2
1007038	MS10-070: Vulnerability in ASP.NET Could Allow Information Disclosure - Microsoft .NET Framework 3.5 - Windows XP SP2 / Windows Server 2003 SP2 / Windows Vista SP2 / Windows Server 2008 SP2 (x64)

1007043	MS10-070: Vulnerability in ASP.NET Could Allow Information Disclosure - Microsoft .NET Framework 2.0 SP2 / 3.5 SP1 - Windows Vista SP1 / Windows Server 2008 Gold (x64)
1007403	MS10-074: Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution - Windows XP SP2 (x64)
1007404	MS10-074: Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1007409	MS10-074: Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution - Windows Vista SP1/SP2
1007411	MS10-074: Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution - Windows Vista SP1/SP2 (x64)
1007417	MS10-074: Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution - Windows 7
1007419	MS10-074: Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution - Windows 7 (x64)
1007501	MS10-075: Vulnerability in Media Player Network Sharing Service Could Allow Remote Code Execution - Windows Vista SP1/SP2
1007503	MS10-075: Vulnerability in Media Player Network Sharing Service Could Allow Remote Code Execution - Windows Vista SP1/SP2 (x64)
1007505	MS10-075: Vulnerability in Media Player Network Sharing Service Could Allow Remote Code Execution - Windows 7
1007507	MS10-075: Vulnerability in Media Player Network Sharing Service Could Allow Remote Code Execution - Windows 7 (x64)
1007603	MS10-076: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution - Windows XP SP2 (x64)
1007604	MS10-076: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1007609	MS10-076: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution - Windows Vista SP1/SP2
1007611	MS10-076: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution - Windows Vista SP1/SP2 (x64)
1007617	MS10-076: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution - Windows 7
1007619	MS10-076: Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution - Windows 7 (x64)
1007903	MS10-079: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution - Office XP SP3 (Administrative Installation)
1008109	MS10-081: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution - Windows Vista SP1/SP2
1008111	MS10-081: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution - Windows Vista SP1/SP2 (x64)

1008117	MS10-081: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution - Windows 7
1008119	MS10-081: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution - Windows 7 (x64)
1008203	MS10-082: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Windows Media Player 10/11 - Windows XP SP2 (x64)
1008209	MS10-082: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Windows Media Player 11 - Windows Vista SP1
1008211	MS10-082: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Windows Media Player 11 - Windows Vista SP1 (x64)
1008217	MS10-082: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Windows Media Player 12 - Windows 7
1008219	MS10-082: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Windows Media Player 12 - Windows 7 (x64)
1008303	MS10-083: Vulnerability in COM Validation in Windows Shell and WordPad Could Allow Remote Code Execution - Windows XP SP2 (x64)
1008304	MS10-083: Vulnerability in COM Validation in Windows Shell and WordPad Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1008309	MS10-083: Vulnerability in COM Validation in WordPad Could Allow Remote Code Execution - Windows Vista SP1/SP2
1008311	MS10-083: Vulnerability in COM Validation in WordPad Could Allow Remote Code Execution - Windows Vista SP1/SP2 (x64)
1008317	MS10-083: Vulnerability in COM Validation in WordPad Could Allow Remote Code Execution - Windows 7
1008319	MS10-083: Vulnerability in COM Validation in WordPad Could Allow Remote Code Execution - Windows 7 (x64)
1008323	MS10-083: Vulnerability in COM Validation in Windows Shell Could Allow Remote Code Execution - Windows Vista SP1/SP2
1008325	MS10-083: Vulnerability in COM Validation in Windows Shell Could Allow Remote Code Execution - Windows Vista SP1/SP2 (x64)
1008331	MS10-083: Vulnerability in COM Validation in Windows Shell Could Allow Remote Code Execution - Windows 7
1008333	MS10-083: Vulnerability in COM Validation in Windows Shell Could Allow Remote Code Execution - Windows 7 (x64)
1008501	MS10-085: Vulnerability in SChannel Could Allow Denial of Service - Windows Vista SP1
1008503	MS10-085: Vulnerability in SChannel Could Allow Denial of Service - Windows Vista SP1 (x64)
1009201	MS10-092: Vulnerability in Task Scheduler Could Allow Elevation of Privilege - Windows Vista SP1/SP2
1009203	MS10-092: Vulnerability in Task Scheduler Could Allow Elevation of Privilege - Windows Vista SP1/SP2 (x64)

1009209	MS10-092: Vulnerability in Task Scheduler Could Allow Elevation of Privilege - Windows 7
1009211	MS10-092: Vulnerability in Task Scheduler Could Allow Elevation of Privilege - Windows 7 (x64)
1009301	MS10-093: Vulnerability in Windows Movie Maker Could Allow Remote Code Execution - Movie Maker 2.6 - Windows Vista SP1/SP2
1009303	MS10-093: Vulnerability in Windows Movie Maker Could Allow Remote Code Execution - Movie Maker 2.6 - Windows Vista SP1/SP2 (x64)
1009403	MS10-094: Vulnerability in Windows Media Encoder Could Allow Remote Code Execution - Windows Media Encoder 9 (32-bit) - Windows XP SP2/Windows Server 2003 SP2 (x64)
1009404	MS10-094: Vulnerability in Windows Media Encoder Could Allow Remote Code Execution - Windows Media Encoder 9 (32-bit) - Windows XP SP2/Windows Server 2003 SP2 (x64) - CORRUPT PATCH
1009405	MS10-094: Vulnerability in Windows Media Encoder Could Allow Remote Code Execution - Windows Media Encoder 9 (64-bit) - Windows XP SP2/Windows Server 2003 SP2 (x64)
1009406	MS10-094: Vulnerability in Windows Media Encoder Could Allow Remote Code Execution - Windows Media Encoder 9 (64-bit) - Windows XP SP2/Windows Server 2003 SP2 (x64) - CORRUPT PATCH
1009407	MS10-094: Vulnerability in Windows Media Encoder Could Allow Remote Code Execution - Windows Media Encoder 9 (32-bit) - Windows Vista SP1/SP2
1009408	MS10-094: Vulnerability in Windows Media Encoder Could Allow Remote Code Execution - Windows Media Encoder 9 (32-bit) - Windows Vista SP1/SP2 - CORRUPT PATCH
1009409	MS10-094: Vulnerability in Windows Media Encoder Could Allow Remote Code Execution - Windows Media Encoder 9 (32-bit) - Windows Vista SP1/SP2 (x64)
1009410	MS10-094: Vulnerability in Windows Media Encoder Could Allow Remote Code Execution - Windows Media Encoder 9 (32-bit) - Windows Vista SP1/SP2 (x64) - CORRUPT PATCH
1009411	MS10-094: Vulnerability in Windows Media Encoder Could Allow Remote Code Execution - Windows Media Encoder 9 (64-bit) - Windows Vista SP1/SP2 (x64)
1009412	MS10-094: Vulnerability in Windows Media Encoder Could Allow Remote Code Execution - Windows Media Encoder 9 (64-bit) - Windows Vista SP1/SP2 (x64) - CORRUPT PATCH
1009603	MS10-096: Vulnerability in Windows Address Book Could Allow Remote Code Execution - Windows XP SP2 (x64)
1009604	MS10-096: Vulnerability in Windows Address Book Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1009609	MS10-096: Vulnerability in Windows Address Book Could Allow Remote Code Execution - Windows Vista SP1/SP2

1009611	MS10-096: Vulnerability in Windows Address Book Could Allow Remote Code Execution - Windows Vista SP1/SP2 (x64)
1009617	MS10-096: Vulnerability in Windows Address Book Could Allow Remote Code Execution - Windows 7
1009619	MS10-096: Vulnerability in Windows Address Book Could Allow Remote Code Execution - Windows 7 (x64)
1009703	MS10-097: Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution - Windows XP SP2 (x64)
1009704	MS10-097: Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1010001	MS10-100: Vulnerability in Consent User Interface Could Allow Elevation of Privilege - Windows Vista SP1
1010003	MS10-100: Vulnerability in Consent User Interface Could Allow Elevation of Privilege - Windows Vista SP1 (x64)
1010009	MS10-100: Vulnerability in Consent User Interface Could Allow Elevation of Privilege - Windows 7
1010011	MS10-100: Vulnerability in Consent User Interface Could Allow Elevation of Privilege - Windows 7 (x64)
1010301	MS10-103: Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution - Microsoft Publisher 2002 SP3 - Office XP SP3 (Local/Network Installation)
1010303	MS10-103: Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution - Microsoft Publisher 2002 SP3 - Office XP SP3 (Administrative Installation)
1010503	MS10-105: Vulnerabilities in Microsoft Office Graphics Filters Could Allow for Remote Code Execution - Office XP SP3 (Administrative Installation)
1100101	MS11-001: Vulnerability in Windows Backup Manager Could Allow Remote Code Execution - Windows Vista SP1/SP2
1100103	MS11-001: Vulnerability in Windows Backup Manager Could Allow Remote Code Execution - Windows Vista SP1/SP2 (x64)
1100203	MS11-002: Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution - Microsoft Data Access Components 2.8 SP2 - Windows XP SP2 (x64)
1100204	MS11-002: Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution - Microsoft Data Access Components 2.8 SP2 - Windows XP SP2 (x64) - CORRUPT PATCH
1100209	MS11-002: Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution - Windows Data Access Components 6.0 - Windows Vista SP1/SP2
1100211	MS11-002: Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution - Windows Data Access Components 6.0 - Windows Vista SP1/SP2 (x64)

1100217	MS11-002: Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution - Windows Data Access Components 6.0 - Windows 7 Gold
1100219	MS11-002: Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution - Windows Data Access Components 6.0 - Windows 7 (x64)
1100401	MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution - FTP 7.0 - Windows Vista SP1
1100402	MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution - FTP 7.5 - Windows Vista SP1
1100405	MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution - FTP 7.0 - Windows Vista SP1 (x64)
1100406	MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution - FTP 7.5 - Windows Vista SP1 (x64)
1100603	MS11-006: Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution - Windows XP SP2 (x64)
1100604	MS11-006: Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1100609	MS11-006: Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution - Windows Vista SP1/SP2
1100611	MS11-006: Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution - Windows Vista SP1/SP2 (x64)
1101103	MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege - Windows XP SP2 (x64)
1101104	MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege - Windows XP SP2 (x64) - CORRUPT PATCH
1101109	MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege - Windows Vista SP1
1101111	MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege - Windows Vista SP1 (x64)
1101117	MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege - Windows 7 Gold
1101119	MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege - Windows 7 Gold (x64)
1101303	MS11-013: Vulnerabilities in Kerberos Could Allow Elevation of Privilege - Windows XP SP2 (x64)
1101304	MS11-013: Vulnerabilities in Kerberos Could Allow Elevation of Privilege - Windows XP SP2 (x64) - CORRUPT PATCH

1101403	MS11-014: Vulnerability in Local Security Authority Subsystem Service Could Allow Local Elevation of Privilege - Windows XP SP2 (x64)
1101404	MS11-014: Vulnerability in Local Security Authority Subsystem Service Could Allow Local Elevation of Privilege - Windows XP SP2 (x64) - CORRUPT PATCH
1101505	MS11-015: Vulnerabilities in Windows Media Could Allow Remote Code Execution - Windows XP SP2 (x64)
1101506	MS11-015: Vulnerabilities in Windows Media Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1101507	MS11-015: Vulnerabilities in Windows Media Could Allow Remote Code Execution - Windows Vista SP1/SP2
1101509	MS11-015: Vulnerabilities in Windows Media Could Allow Remote Code Execution - Windows Vista SP1/SP2 (x64)
1101511	MS11-015: Vulnerabilities in Windows Media Could Allow Remote Code Execution - Windows 7 Gold/SP1
1101513	MS11-015: Vulnerabilities in Windows Media Could Allow Remote Code Execution - Windows 7 Gold/SP1 (x64)
1101517	MS11-015: Vulnerabilities in Windows Media Could Allow Remote Code Execution - Windows Media Center TV Pack - Windows Vista SP1/SP2
1101519	MS11-015: Vulnerabilities in Windows Media Could Allow Remote Code Execution - Windows Media Center TV Pack -Windows Vista SP1/SP2 (x64)
1101705	MS11-017: Vulnerability in Remote Desktop Client Could Allow Remote Code Execution - Remote Desktop Connection 6.0 Client - Windows XP SP2 (x64)
1101706	MS11-017: Vulnerability in Remote Desktop Client Could Allow Remote Code Execution - Remote Desktop Connection 6.0 Client - Windows XP SP2 (x64) - CORRUPT PATCH
1101713	MS11-017: Vulnerability in Remote Desktop Client Could Allow Remote Code Execution - Remote Desktop Connection 6.1 Client - Windows Vista SP1/SP2
1101715	MS11-017: Vulnerability in Remote Desktop Client Could Allow Remote Code Execution - Remote Desktop Connection 6.1 Client - Windows Vista SP1/SP2 (x64)
1101723	MS11-017: Vulnerability in Remote Desktop Client Could Allow Remote Code Execution - Remote Desktop Connection 7.0 Client - Windows Vista SP1/SP2
1101725	MS11-017: Vulnerability in Remote Desktop Client Could Allow Remote Code Execution - Remote Desktop Connection 7.0 Client - Windows Vista SP1/SP2 (x64)
1101727	MS11-017: Vulnerability in Remote Desktop Client Could Allow Remote Code Execution - Remote Desktop Connection 7.0 Client - Windows 7 Gold

1101729	MS11-017: Vulnerability in Remote Desktop Client Could Allow Remote Code Execution - Remote Desktop Connection 7.0 Client - Windows 7 Gold (x64)
1101910	MS11-019: Vulnerabilities in SMB Client Could Allow Remote Code Execution - Windows Vista SP1/SP2
1101911	MS11-019: Vulnerabilities in SMB Client Could Allow Remote Code Execution - Windows 7 Gold/SP1
1101912	MS11-019: Vulnerabilities in SMB Client Could Allow Remote Code Execution - Windows Vista SP1/SP2 (x64)
1101913	MS11-019: Vulnerabilities in SMB Client Could Allow Remote Code Execution - Windows 7 Gold/SP1 (x64)
1102005	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution - Windows XP SP2 (x64)
1102006	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1102011	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution - Windows Vista SP1
1102013	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution - Windows Vista SP1 (x64)
1102303	MS11-023: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution - Office XP SP3 (Administrative Installation)
1102405	MS11-024: Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution - Windows XP SP2 (KB2491683) (x64)
1102406	MS11-024: Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution - Windows XP SP2 (KB2491683) (x64) - CORRUPT PATCH
1102407	MS11-024: Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution - Windows XP SP2 (KB2506212) (x64)
1102408	MS11-024: Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution - Windows XP SP2 (KB2506212) (x64) - CORRUPT PATCH
1102417	MS11-024: Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution - Windows Vista SP1/SP2 (KB2491683)
1102419	MS11-024: Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution - Windows Vista SP1/SP2 (KB2506212)
1102421	MS11-024: Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution - Windows Vista SP1/SP2 (KB2491683) (x64)
1102423	MS11-024: Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution - Windows Vista SP1/SP2 (KB2506212) (x64)
1102433	MS11-024: Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution - Windows 7 Gold/SP1 (KB2491683)
1102435	MS11-024: Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution - Windows 7 Gold/SP1 (KB2506212)

1102437	MS11-024: Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution - Windows 7 Gold/SP1 (KB2491683) (x64)
1102439	MS11-024: Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution - Windows 7 Gold/SP1 (KB2506212) (x64)
1102709	MS11-027: Cumulative Security Update of ActiveX Kill Bits - Windows Vista SP1
1102711	MS11-027: Cumulative Security Update of ActiveX Kill Bits - Windows Vista SP1 (x64)
1102909	MS11-029: Vulnerability in GDI+ Could Allow Remote Code Execution - Windows Vista SP1
1102912	MS11-029: Vulnerability in GDI+ Could Allow Remote Code Execution - Windows Vista SP1 (x64)
1102918	MS11-029: Vulnerability in GDI+ Could Allow Remote Code Execution - Office XP SP3 (Administrative Installation)
1103005	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution - Windows Vista SP1/SP2
1103007	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution - Windows Vista SP1/SP2 (x64)
1103011	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution - Windows 7 Gold/SP1
1103012	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1103013	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution - Windows 7 Gold/SP1 (x64)
1103105	MS11-031: Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution - JScript 5.6 and VBScript 5.6 - Windows XP SP2 (x64)
1103106	MS11-031: Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution - JScript 5.6 and VBScript 5.6 - Windows XP SP2 (x64) - CORRUPT PATCH
1103107	MS11-031: Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution - JScript 5.7 and VBScript 5.7 - Windows XP SP2 (x64)
1103108	MS11-031: Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution - JScript 5.7 and VBScript 5.7 - Windows XP SP2 (x64) - CORRUPT PATCH
1103123	MS11-031: Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution - JScript 5.7 and VBScript 5.7 - Windows Vista SP1
1103125	MS11-031: Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution - JScript 5.8 and VBScript 5.8 - Windows Vista SP1/SP2

1103127	MS11-031: Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution - JScript 5.7 and VBScript 5.7 - Windows Vista SP1 (x64)
1103139	MS11-031: Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution - JScript 5.8 and VBScript 5.8 - Windows 7 Gold/SP1
1103209	MS11-032: Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution - Windows Vista SP1
1103211	MS11-032: Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution - Windows Vista SP1 (x64)
1103303	MS11-033: Vulnerability in WordPad Text Converters Could Allow Remote Code Execution - Windows XP SP2 (x64)
1103304	MS11-033: Vulnerability in WordPad Text Converters Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1103601	MS11-036: Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution - Office XP SP3 (Local/Network Installation) (Superseded)
1103603	MS11-036: Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution - Office XP SP3 (Administrative Installation)
1103709	MS11-037: Vulnerability in MHTML Could Allow Information Disclosure - Windows Vista SP1
1103711	MS11-037: Vulnerability in MHTML Could Allow Information Disclosure - Windows Vista SP1 (x64)
1103717	MS11-037: Vulnerability in MHTML Could Allow Information Disclosure - Windows 7 Gold/SP1
1103719	MS11-037: Vulnerability in MHTML Could Allow Information Disclosure - Windows 7 Gold/SP1 (x64)
1103727	MS11-037: Vulnerability in MHTML Could Allow Information Disclosure - Windows XP SP2 (x64) (v2
1103728	MS11-037: Vulnerability in MHTML Could Allow Information Disclosure - Windows XP SP2 (x64) (v2
1103803	MS11-038: Vulnerability in OLE Automation Could Allow Remote Code Execution - Windows XP SP2 (x64)
1103804	MS11-038: Vulnerability in OLE Automation Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1103809	MS11-038: Vulnerability in OLE Automation Could Allow Remote Code Execution - Windows Vista SP1
1103811	MS11-038: Vulnerability in OLE Automation Could Allow Remote Code Execution - Windows Vista SP1 (x64)
1103901	MS11-039: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution - Microsoft .NET Framework 3.5 - Windows XP SP3 / 2003 SP2

1103907	MS11-039: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution - Microsoft .NET Framework 3.5 - Windows XP SP2 / 2003 SP2 (x64)
1103913	MS11-039: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution - Microsoft .NET Framework 2.0 SP1 / 3.5 - Windows Vista SP1 / 2008 Gold
1103915	MS11-039: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution - Microsoft .NET Framework 2.0 SP2 / Microsoft .NET Framework 3.5 SP1 - Windows Vista SP1 / Windows Server 2008
1103919	MS11-039: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution - Microsoft .NET Framework 2.0 SP1 / 3.5 - Windows Vista SP1 / 2008 Gold (x64)
1103921	MS11-039: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution - Microsoft .NET Framework 2.0 SP2 / 3.5 SP1 - Windows Vista SP1 / 2008 Gold (x64)
1104203	MS11-042: Vulnerabilities in Distributed File System Could Allow Remote Code Execution - Windows XP SP2 (x64)
1104204	MS11-042: Vulnerabilities in Distributed File System Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1104209	MS11-042: Vulnerabilities in Distributed File System Could Allow Remote Code Execution - Windows Vista SP1
1104211	MS11-042: Vulnerabilities in Distributed File System Could Allow Remote Code Execution - Windows Vista SP1 (x64)
1104217	MS11-042: Vulnerabilities in Distributed File System Could Allow Remote Code Execution - Windows 7 Gold
1104219	MS11-042: Vulnerabilities in Distributed File System Could Allow Remote Code Execution - Windows 7 Gold (x64)
1104325	MS11-043: Vulnerability in SMB Client Could Allow Remote Code Execution - Windows Server 2003 SP2 (v2, republished 8/9/2011)
1104326	MS11-043: Vulnerability in SMB Client Could Allow Remote Code Execution - Windows Server 2003 SP2 (v2, republished 8/9/2011) - CORRUPT PATCH
1104327	MS11-043: Vulnerability in SMB Client Could Allow Remote Code Execution - Windows Vista SP1 (v2, republished 8/9/2011)
1104329	MS11-043: Vulnerability in SMB Client Could Allow Remote Code Execution - Windows Server 2008 Gold (v2, republished 8/9/2011)
1104333	MS11-043: Vulnerability in SMB Client Could Allow Remote Code Execution - Windows XP SP2 (x64) (v2, republished 8/9/2011)
1104334	MS11-043: Vulnerability in SMB Client Could Allow Remote Code Execution - Windows XP SP2 (x64) (v2, republished 8/9/2011) - CORRUPT PATCH
1104335	MS11-043: Vulnerability in SMB Client Could Allow Remote Code Execution - Windows Server 2003 SP2 (x64) (v2, republished 8/9/2011)

1104336	MS11-043: Vulnerability in SMB Client Could Allow Remote Code Execution - Windows Server 2003 SP2 (x64) (v2, republished 8/9/2011) - CORRUPT PATCH
1104337	MS11-043: Vulnerability in SMB Client Could Allow Remote Code Execution - Windows Vista SP1 (x64) (v2, republished 8/9/2011)
1104339	MS11-043: Vulnerability in SMB Client Could Allow Remote Code Execution - Windows Server 2008 Gold (x64) (v2, republished 8/9/2011)
1104403	MS11-044: Vulnerability in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 2.0 SP1 / 3.5 Gold - Windows XP SP3 and Windows Server 2003 SP2
1104409	MS11-044: Vulnerability in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 2.0 SP1 / 3.5 Gold - Windows XP SP2 and Windows Server 2003 SP2 (x64)
1104413	MS11-044: Vulnerability in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 2.0 SP1 / 3.5 - Windows Vista SP1 and Windows Server 2008
1104415	MS11-044: Vulnerability in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 2.0 SP2 / 3.5 SP1 - Windows Vista SP1 and Windows Server 2008
1104419	MS11-044: Vulnerability in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 2.0 SP1 / 3.5 - Windows Vista SP1 and Windows Server 2008 (x64)
1104421	MS11-044: Vulnerability in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 2.0 SP2 / 3.5 SP1 - Windows Vista SP1 / Windows Server 2008 (x64)
1104503	MS11-045: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution - Microsoft Excel 2002 SP3 - Office XP SP3 (Administrative Installation)
1104609	MS11-046: Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege - Windows Vista SP1
1104611	MS11-046: Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege - Windows Vista SP1 (x64)
1104617	MS11-046: Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege - Windows 7 Gold
1104801	MS11-048: Vulnerability in SMB Server Could Allow Denial of Service - Windows Vista SP1
1104803	MS11-048: Vulnerability in SMB Server Could Allow Denial of Service - Windows Vista SP1 (x64)
1105301	MS11-053: Vulnerability in Bluetooth Stack Could Allow Remote Code Execution - Windows Vista SP1
1105303	MS11-053: Vulnerability in Bluetooth Stack Could Allow Remote Code Execution - Windows Vista SP2
1105305	MS11-053: Vulnerability in Bluetooth Stack Could Allow Remote Code Execution - Windows Vista SP1 (x64)

1105307	MS11-053: Vulnerability in Bluetooth Stack Could Allow Remote Code Execution - Windows Vista SP2 (x64)
1105309	MS11-053: Vulnerability in Bluetooth Stack Could Allow Remote Code Execution - Windows 7 Gold/SP1
1105311	MS11-053: Vulnerability in Bluetooth Stack Could Allow Remote Code Execution - Windows 7 Gold/SP1 (x64)
1105409	MS11-054: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege - Windows Vista SP1
1105411	MS11-054: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege - Windows Vista SP1 (x64)
1105603	MS11-056: Vulnerabilities in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege - Windows XP SP2 (x64)
1105604	MS11-056: Vulnerabilities in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege - Windows XP SP2 (x64) - CORRUPT PATCH
1105609	MS11-056: Vulnerabilities in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege - Windows Vista SP1/SP2
1105611	MS11-056: Vulnerabilities in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege - Windows Vista SP1/SP2 (x64)
1105901	MS11-059: Vulnerability in Data Access Components Could Allow Remote Code Execution - Windows 7 Gold/SP1
1105903	MS11-059: Vulnerability in Data Access Components Could Allow Remote Code Execution - Windows 7 Gold/SP1 (x64)
1106203	MS11-062: Vulnerability in Remote Access Service NDISTAPI Driver Could Allow Elevation of Privilege - Windows XP SP2 (x64)
1106204	MS11-062: Vulnerability in Remote Access Service NDISTAPI Driver Could Allow Elevation of Privilege - Windows XP SP2 (x64) - CORRUPT PATCH
1106601	MS11-066: Vulnerability in Microsoft Chart Control Could Allow Information Disclosure - Microsoft .NET Framework 4 - Windows XP SP3 / 2003 SP2 / Vista SP2 / 2008 SP2 / 7 Gold/SP1
1106603	MS11-066: Vulnerability in Microsoft Chart Control Could Allow Information Disclosure - Microsoft .NET Framework 4 - Windows XP SP2 / 2003 SP2 / Vista SP2 /2008 SP2 / 7 Gold/SP1 / 2008 R2 Gold/SP1 (x64)
1106605	MS11-066: Vulnerability in Microsoft Chart Control Could Allow Information Disclosure - Chart Control for Microsoft .NET Framework 3.5 SP1
1107103	MS11-071: Vulnerability in Windows Components Could Allow Remote Code Execution - Windows XP SP2 (x64)
1107109	MS11-071: Vulnerability in Windows Components Could Allow Remote Code Execution - Windows Vista SP2

1107111	MS11-071: Vulnerability in Windows Components Could Allow Remote Code Execution - Windows Vista SP2 (x64)
1107117	MS11-071: Vulnerability in Windows Components Could Allow Remote Code Execution - Windows 7 Gold/SP1
1107119	MS11-071: Vulnerability in Windows Components Could Allow Remote Code Execution - Windows 7 Gold/SP1 (x64)
1107503	MS11-075: Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution - Windows XP SP2 (x64)
1107504	MS11-075: Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1107509	MS11-075: Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution - Windows Vista SP2
1107511	MS11-075: Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution - Windows Vista SP2 (x64)
1107517	MS11-075: Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution - Windows 7 Gold/SP1
1107519	MS11-075: Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution - Windows 7 Gold/SP1 (x64)
1107601	MS11-076: Vulnerability in Windows Media Center Could Allow Remote Code Execution - Windows Vista SP2
1107603	MS11-076: Vulnerability in Windows Media Center Could Allow Remote Code Execution - Windows Vista SP2 (x64)
1107605	MS11-076: Vulnerability in Windows Media Center Could Allow Remote Code Execution - Windows 7 Gold/SP1
1107607	MS11-076: Vulnerability in Windows Media Center Could Allow Remote Code Execution - Windows 7 Gold/SP1 (x64)
1107609	MS11-076: Vulnerability in Windows Media Center Could Allow Remote Code Execution - Windows Media Center TV Pack - Windows Vista SP2
1107611	MS11-076: Vulnerability in Windows Media Center Could Allow Remote Code Execution - Windows Media Center TV Pack - Windows Vista SP2 (x64)
1108509	MS11-085: Vulnerability in Windows Mail and Windows Meeting Space Could Allow Remote Code Execution - Windows 7 Gold/SP1
1108511	MS11-085: Vulnerability in Windows Mail and Windows Meeting Space Could Allow Remote Code Execution - Windows 7 Gold/SP1 (x64)
1109205	MS11-092: Vulnerability in Windows Media Could Allow Remote Code Execution - Windows XP SP2 (x64)
1109206	MS11-092: Vulnerability in Windows Media Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1109207	MS11-092: Vulnerability in Windows Media Could Allow Remote Code Execution - Windows Vista SP2
1109209	MS11-092: Vulnerability in Windows Media Could Allow Remote Code Execution - Windows Vista SP2 (x64)

1109211	MS11-092: Vulnerability in Windows Media Could Allow Remote Code Execution - Windows 7 Gold/SP1
1109213	MS11-092: Vulnerability in Windows Media Could Allow Remote Code Execution - Windows 7 Gold/SP1 (x64)
1109703	MS11-097: Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege - Windows XP SP2 (x64)
1109704	MS11-097: Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege - Windows XP SP2 (x64) - CORRUPT PATCH
1110007	MS11-100: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Microsoft .NET Framework 4 - Windows 7 Gold
1110013	MS11-100: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Microsoft .NET Framework 4.0 - Windows 7 Gold / 2008 R2 Gold (x64)
1110021	MS11-100: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Microsoft .NET Framework 3.5 SP1 - Windows 7 Gold
1110023	MS11-100: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Microsoft .NET Framework 3.5 SP1 - Windows 7 SP1
1110025	MS11-100: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Microsoft .NET Framework 3.5.1 - Windows 7 Gold / 2008 R2 Gold (x64)
1110027	MS11-100: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Microsoft .NET Framework 3.5.1 - Windows 7 SP1 / 2008 R2 SP1 (x64)
1200101	MS12-001: Vulnerability in Windows Kernel Could Allow Security Feature Bypass - Windows XP SP2 (x64)
1200102	MS12-001: Vulnerability in Windows Kernel Could Allow Security Feature Bypass - Windows XP SP2 (x64) - CORRUPT PATCH
1200203	MS12-002: Vulnerability in Windows Object Packager Could Allow Remote Code Execution - Windows XP SP2 (x64)
1200407	MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution - Windows Multimedia Library - Windows XP SP2 (x64)
1200408	MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution - Windows Multimedia Library - Windows XP SP2 (x64) - CORRUPT PATCH
1200409	MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution - DirectShow - Windows XP SP2 (x64)
1200410	MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution - DirectShow - Windows XP SP2 (x64) - CORRUPT PATCH
1200419	MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution - Windows Multimedia Library - Windows Vista SP2
1200421	MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution - DirectShow - Windows Vista SP2

1200423	MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution - Windows Multimedia Library - Windows Vista SP2 (x64)
1200425	MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution - DirectShow - Windows Vista SP2 (x64)
1200435	MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution - DirectShow - Windows 7 Gold/SP1
1200437	MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution - DirectShow - Windows 7 Gold/SP1 (x64)
1200441	MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution - Windows Media Center TV Pack - Windows Vista SP1/SP2
1200443	MS12-004: Vulnerabilities in Windows Media Could Allow Remote Code Execution - Windows Media Center TV Pack - Windows Vista SP1/SP2 (x64)
1200503	MS12-005: Vulnerability in Microsoft Windows Could Allow Remote Code Execution - Windows XP SP2 (x64)
1200504	MS12-005: Vulnerability in Microsoft Windows Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1200605	MS12-006: Vulnerability in SSL/TLS Could Allow Information Disclosure - Windows XP SP2 (KB2638806) (x64)
1200615	MS12-006: Vulnerability in SSL/TLS Could Allow Information Disclosure - Windows Vista SP2
1200617	MS12-006: Vulnerability in SSL/TLS Could Allow Information Disclosure - Windows Vista SP2 (x64)
1200623	MS12-006: Vulnerability in SSL/TLS Could Allow Information Disclosure - Windows 7 Gold/SP1
1200625	MS12-006: Vulnerability in SSL/TLS Could Allow Information Disclosure - Windows 7 Gold/SP1 (x64)
1201301	MS12-013: Vulnerability in C Run-Time Library Could Allow Remote Code Execution - Windows Vista SP2
1201303	MS12-013: Vulnerability in C Run-Time Library Could Allow Remote Code Execution - Windows Vista SP2 (x64)
1201309	MS12-013: Vulnerability in C Run-Time Library Could Allow Remote Code Execution - Windows 7 Gold/SP1
1201311	MS12-013: Vulnerability in C Run-Time Library Could Allow Remote Code Execution - Windows 7 Gold/SP1 (x64)
1202009	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution - Windows Vista SP2
1202011	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution - Windows Vista SP2 (x64)
1202017	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution - Windows 7 Gold/SP1 (KB2621440)
1202021	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution - Windows 7 Gold/SP1 (KB2621440) (x64)

1202047	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution - Windows 7 Gold/SP1 (KB2667402) - V2.0
1202051	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution - Windows 7 Gold/SP1 (KB2667402) (x64) - V2.0
1202201	MS12-022: Vulnerability in Expression Design Could Allow Remote Code Execution - Expression Design
1202203	MS12-022: Vulnerability in Expression Design Could Allow Remote Code Execution - Expression Design SP1
1202205	MS12-022: Vulnerability in Expression Design Could Allow Remote Code Execution - Expression Design 2
1202207	MS12-022: Vulnerability in Expression Design Could Allow Remote Code Execution - Expression Design 3
1202209	MS12-022: Vulnerability in Expression Design Could Allow Remote Code Execution - Expression Design 4
1202403	MS12-024: Vulnerability in Windows Could Allow Remote Code Execution - Windows XP SP2 (x64)
1202404	MS12-024: Vulnerability in Windows Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1202409	MS12-024: Vulnerability in Windows Could Allow Remote Code Execution - Windows Vista SP2
1202411	MS12-024: Vulnerability in Windows Could Allow Remote Code Execution - Windows Vista SP2 (x64)
1202417	MS12-024: Vulnerability in Windows Could Allow Remote Code Execution - Windows 7 Gold/SP1
1202419	MS12-024: Vulnerability in Windows Could Allow Remote Code Execution - Windows 7 Gold/SP1 (x64)
1203301	MS12-033: Vulnerability in Windows Partition Manager Could Allow Elevation of Privilege - Windows Vista SP2
1203303	MS12-033: Vulnerability in Windows Partition Manager Could Allow Elevation of Privilege - Windows Vista SP2 (x64)
1203309	MS12-033: Vulnerability in Windows Partition Manager Could Allow Elevation of Privilege - Windows 7 Gold/SP1
1203311	MS12-033: Vulnerability in Windows Partition Manager Could Allow Elevation of Privilege - Windows 7 Gold/SP1 (x64)
1203409	(MS12-034: Combined Security Update for Microsoft Office
1203410	(MS12-034: Combined Security Update for Microsoft Office
1203411	(MS12-034: Combined Security Update for Microsoft Office
1203412	(MS12-034: Combined Security Update for Microsoft Office
1203413	(MS12-034: Combined Security Update for Microsoft Office
1203433	MS12-034: Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight - Windows Vista SP2 (KB2676562)
1203441	MS12-034: Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight - Windows Vista SP2 (x64) (KB2676562)

1203465	MS12-034: Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight - Windows 7 Gold (KB2676562)
1203473	MS12-034: Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight - Windows 7 Gold (x64) (KB2676562)
1203491	MS12-034: Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight - Microsoft .NET Framework 3.5.1 - Windows 7 Gold
1203495	MS12-034: Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight - Microsoft .NET Framework 3.5.1 - Windows 7 / Windows Server 2008 R2 Gold (x64)
1203503	MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 1.1 SP1 - Windows XP SP2 / Windows Server 2003 SP2 / Windows Vista SP2 / Windows Server 2008 SP2 (x64)
1203505	MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 2.0 SP2 - Windows XP SP3 / Windows Server 2003 SP2
1203509	MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 3.5 SP1 - Windows XP SP3 / Windows Server 2003 SP2 / Windows Vista SP2 / Windows Server 2008 SP2
1203511	MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 4 - Windows XP SP3 / 2003 SP2 / Vista SP2 / 2008 SP2 / 7 Gold/SP1
1203513	MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 2.0 SP2 - Windows XP SP2 / Windows Server 2003 SP2 (x64)
1203517	MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 3.5 SP1 - Windows XP SP2 / 2003 SP2 / Vista SP2 / 2008 SP2 (x64)
1203519	MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 4 - Windows XP SP2 / 2003 SP2 / Vista SP2 / 2008 SP2 / 7 Gold/SP1 (x64)
1203523	MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 2.0 SP2 - Windows Vista SP2 / Windows Server 2008 SP2
1203527	MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 2.0 SP2 - Windows Vista SP2 / Windows Server 2008 SP2 (x64)
1203531	MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 3.5.1 - Windows 7 Gold
1203533	MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 3.5.1 - Windows 7 SP1

1203535	MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 3.5.1 - Windows 7 Gold / Windows Server 2008 R2 Gold (x64)
1203537	MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Microsoft .NET Framework 3.5.1 - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)
1203539	MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 1.1 SP1 - Windows XP SP3 / Windows Vista SP2 / Windows Server 2008 SP2
1203603	MS12-036: Vulnerability in Remote Desktop Could Allow Remote Code Execution - Windows XP SP2(x64)
1203604	MS12-036: Vulnerability in Remote Desktop Could Allow Remote Code Execution - Windows XP SP2(x64) - CORRUPT PATCH
1203609	MS12-036: Vulnerability in Remote Desktop Could Allow Remote Code Execution - Windows Vista SP2
1203611	MS12-036: Vulnerability in Remote Desktop Could Allow Remote Code Execution - Windows Vista SP2 (x64)
1203617	MS12-036: Vulnerability in Remote Desktop Could Allow Remote Code Execution - Windows 7 Gold/SP1
1203619	MS12-036: Vulnerability in Remote Desktop Could Allow Remote Code Execution - Windows 7 Gold/SP1 (x64)
1204325	MS12-043: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution - Microsoft XML Core Services 3.0 / 6.0 - Windows 7 Gold
1204503	MS12-045: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution - Microsoft Data Access Components 2.8 SP2 - Windows XP SP2 (x64)
1204504	MS12-045: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution - Microsoft Data Access Components 2.8 SP2 - Windows XP SP2 (x64) - CORRUPT PATCH
1204509	MS12-045: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution - Windows Data Access Components 6.0 - Windows Vista SP2
1204511	MS12-045: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution - Windows Data Access Components 6.0 - Windows Vista SP2 (x64)
1204517	MS12-045: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution - Windows Data Access Components 6.0 - Windows 7 Gold/SP1
1204519	MS12-045: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution - Windows Data Access Components 6.0 - Windows 7 Gold/SP1 (x64)
1204803	MS12-048: Vulnerability in Windows Shell Could Allow Remote Code Execution - Windows XP SP2 (x64)

1204804	MS12-048: Vulnerability in Windows Shell Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1204817	MS12-048: Vulnerability in Windows Shell Could Allow Remote Code Execution - Windows 7 Gold
1204819	MS12-048: Vulnerability in Windows Shell Could Allow Remote Code Execution - Windows 7 Gold (x64)
1204903	MS12-049: Vulnerability in TLS Could Allow Information Disclosure - Windows XP SP2 (x64)
1204904	MS12-049: Vulnerability in TLS Could Allow Information Disclosure - Windows XP SP2 (x64) - CORRUPT PATCH
1204917	MS12-049: Vulnerability in TLS Could Allow Information Disclosure - Windows 7 Gold
1204919	MS12-049: Vulnerability in TLS Could Allow Information Disclosure - Windows 7 Gold (x64)
1205407	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution - Windows XP SP2 (x64) - KB2705219 - V2
1205408	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution - Windows XP SP2 (x64) - KB2712808
1205417	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution - Windows Vista SP2 - KB2705219 - V2
1205421	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution - Windows Vista SP2 (x64) - KB2705219 - V2
1205422	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution - Windows XP SP2 (x64) - KB2705219 - V2 - CORRUPT PATCH
1205424	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution - Windows XP SP2 (x64) - KB2712808 - CORRUPT PATCH
1205433	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution - Windows 7 Gold/SP1 - KB2705219 - V2
1205435	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution - Windows 7 Gold - KB2712808
1205437	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution - Windows 7 Gold/SP1 (x64) - KB2705219 - V2
1205439	MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution - Windows 7 Gold - KB2712808 (x64)
1205601	MS12-056: Vulnerability in JScript and VBScript Engines Could Allow Remote Code Execution - JScript 5.8 and VBScript 5.8 - Windows XP SP2 (x64)

1205602	MS12-056: Vulnerability in JScript and VBScript Engines Could Allow Remote Code Execution - JScript 5.8 and VBScript 5.8 - Windows XP SP2 (x64) - CORRUPT PATCH
1205605	MS12-056: Vulnerability in JScript and VBScript Engines Could Allow Remote Code Execution - JScript 5.8 and VBScript 5.8 - Windows Vista SP2 (x64)
1205609	MS12-056: Vulnerability in JScript and VBScript Engines Could Allow Remote Code Execution - JScript 5.8 and VBScript 5.8 - Windows 7 Gold/SP1 (x64)
1206901	MS12-069: Vulnerability in Kerberos Could Allow Denial of Service - Windows 7 Gold
1206903	MS12-069: Vulnerability in Kerberos Could Allow Denial of Service - Windows 7 Gold (x64)
1207003	MS12-070: Vulnerability in SQL Server Could Allow Elevation of Privilege - SQL Server 2005 Express Edition with Advanced Services SP4 / SQL Server 2005 SP4 - QFE Branch
1207005	MS12-070: Vulnerability in SQL Server Could Allow Elevation of Privilege - SQL Server 2005 Express Edition with Advanced Services SP4 / SQL Server 2005 SP4 - GDR Branch
1207203	MS12-072: Vulnerabilities in Windows Shell Could Allow Remote Code Execution - Windows XP SP2 (x64)
1207204	MS12-072: Vulnerabilities in Windows Shell Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1207209	MS12-072: Vulnerabilities in Windows Shell Could Allow Remote Code Execution - Windows Vista SP2
1207211	MS12-072: Vulnerabilities in Windows Shell Could Allow Remote Code Execution - Windows Vista SP2 (x64)
1207217	MS12-072: Vulnerabilities in Windows Shell Could Allow Remote Code Execution - Windows 7 Gold/SP1
1207219	MS12-072: Vulnerabilities in Windows Shell Could Allow Remote Code Execution - Windows 7 Gold/SP1 (x64)
1207223	MS12-072: Vulnerabilities in Windows Shell Could Allow Remote Code Execution - Windows 8 Gold
1207225	MS12-072: Vulnerabilities in Windows Shell Could Allow Remote Code Execution - Windows 8 Gold (x64)
1207301	MS12-073: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Information Disclosure - FTP Service 7.0 for IIS 7.0 - Windows Vista SP2
1207303	MS12-073: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Information Disclosure - FTP Service 7.5 for IIS 7.0 - Windows Vista SP2
1207305	MS12-073: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Information Disclosure - FTP Service 7.0 for IIS 7.0 - Windows Vista SP2 (x64)

1207307	MS12-073: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Information Disclosure - FTP Service 7.5 for IIS 7.0 - Windows Vista SP2 (x64)
1207317	MS12-073: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Information Disclosure - FTP Service 7.5 for IIS 7.5 - Windows 7 Gold/SP1
1207319	MS12-073: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Information Disclosure - IIS 7.5 - Windows 7 Gold/SP1
1207321	MS12-073: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Information Disclosure - FTP Service 7.5 for IIS 7.5 - Windows 7 Gold/SP1 (x64)
1207323	MS12-073: Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Information Disclosure - IIS 7.5 - Windows 7 Gold/SP1 (x64)
1207405	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 2.0 SP2 - Windows XP SP3 /Server 2003 SP2
1207407	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4 - Windows XP SP3 / Server 2003 SP2 / Vista SP2 / Server 2008 SP2 / 7 Gold/SP1
1207409	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4 - Windows XP SP3 / Server 2003 SP2 / Vista SP2 / Server 2008 SP2 / 7 Gold/SP1 (KB2737019)
1207411	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 2.0 SP2 - Windows XP SP2 / Server 2003 SP2 (x64)
1207413	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4 - Windows XP SP2 / Server 2003 SP2 / Vista SP2 / Server 2008 SP2 / 7 Gold/SP1 / 2008 R2 Gold/SP1 (x64)
1207415	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4 - Windows XP SP3 / 2003 SP2 / Vista SP2 / 2008 SP2 / 7 Gold/SP1 / 2008 R2 Gold/SP1 (x64)
1207419	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 2.0 SP2 - Windows Vista SP2 / Server 2008 SP2
1207423	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4.5 - Windows Vista SP2 / Server 2008 SP2 / 7 SP1
1207425	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 2.0 SP2 - Windows Vista SP2 / Server 2008 SP2 (x64)
1207429	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4.5 - Windows Vista SP2 / 2008 SP2 / 7 SP1 / 2008 R2 SP1 (x64)

1207431	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 3.5.1 - Windows 7 Gold
1207433	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 3.5.1 - Windows 7 SP1
1207435	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 3.5.1 - Windows 7 / Server 2008 R2 Gold (x64)
1207437	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 3.5.1 - Windows 7 SP1 / Server 2008 R2 SP1 (x64)
1207455	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4.5 - Windows 8 (KB2737084)
1207457	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4.5 - Windows 8 / Server 2012 (x64) (KB2737084)
1207459	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4.5 - Windows 8 Gold (KB2756872)
1207461	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4.5 - Windows 8 Gold (KB2761094)
1207463	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4.5 - Windows 8 Gold (KB2764870)
1207465	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4.5 - Windows 8 Gold (x64) (KB2756872)
1207467	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4.5 - Windows 8 Gold (x64) (KB2761094)
1207469	MS12-074: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4.5 - Windows 8 Gold (x64) (KB2764870)
1207833	MS12-078: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - Windows 7 Gold (KB2753842) (V2.0)
1207837	MS12-078: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - Windows 7 Gold (KB2753842) (x64) (V2.0)
1208117	MS12-081: Vulnerability in Windows File Handling Component Could Allow Remote Code Execution - Windows 7 Gold/SP1
1208119	MS12-081: Vulnerability in Windows File Handling Component Could Allow Remote Code Execution - Windows 7 Gold/SP1 (x64)
1208203	MS12-082: Vulnerability in DirectPlay Could Allow Remote Code Execution - Windows XP SP2 (x64)
1208204	MS12-082: Vulnerability in DirectPlay Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1208209	MS12-082: Vulnerability in DirectPlay Could Allow Remote Code Execution - Windows Vista SP2
1208211	MS12-082: Vulnerability in DirectPlay Could Allow Remote Code Execution - Windows Vista SP2 (x64)

1208217	MS12-082: Vulnerability in DirectPlay Could Allow Remote Code Execution - Windows 7 Gold/SP1
1208219	MS12-082: Vulnerability in DirectPlay Could Allow Remote Code Execution - Windows 7 Gold/SP1 (x64)
1208223	MS12-082: Vulnerability in DirectPlay Could Allow Remote Code Execution - Windows 8 Gold
1208225	MS12-082: Vulnerability in DirectPlay Could Allow Remote Code Execution - Windows 8 Gold (x64)
1300101	MS13-001: Vulnerability in Windows Print Spooler Components Could Allow Remote Code Execution - Windows 7 Gold
1300103	MS13-001: Vulnerability in Windows Print Spooler Components Could Allow Remote Code Execution - Windows 7 Gold (x64)
1300201	MS13-002: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 4.0 - Windows XP SP3 / 2003 SP2 / Vista SP2 / 2008 SP2 / 7 Gold/SP1 / 8 Gold
1300207	MS13-002: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 4.0 - XP SP2 / 2003 SP2 / Vista SP2 / 2008 SP2 / 7 Gold/SP1 / 2008 R2 Gold/SP1 / 8 Gold / 2012 Gold (x64)
1300223	MS13-002: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 6.0 - Windows 7 Gold
1300225	MS13-002: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 3.0 / 6.0 - Windows 7 Gold (x64)
1300237	MS13-002: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution - XML Core Services 5.0 - Office 2007 SP2 / Word Viewer / Office Compatibility Pack SP2/SP3 / Expression Web
1300405	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 2.0 SP2 - Windows XP SP3 / Windows Server 2003 SP2
1300407	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4 - Windows XP SP3 / Windows Server 2003 SP2 / Windows Vista SP2 / Windows Server 2008 SP2 / Windows 7 Gold/SP1
1300409	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 3.0 SP2 - Windows XP SP3
1300411	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 2.0 SP2 - Windows XP SP2 / Windows Server 2003 SP2 (x64)
1300413	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4 - Windows XP SP2 / 2003 SP2 / Vista SP2 / 2008 SP2 / 7 Gold/SP1 / 2008 R2 Gold/SP1 (x64)
1300415	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 3.0 SP2 - Windows XP SP2 (x64)

1300419	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 2.0 SP2 - Windows Vista SP2 / Windows Server 2008 SP2
1300421	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4.5 - Windows Vista SP2 / Windows Server 2008 SP2 / Windows 7 SP1
1300425	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 2.0 SP2 - Windows Vista SP2 / Windows Server 2008 SP2 (x64)
1300427	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4.5 - Windows Vista SP2 / 2008 SP2 / 7 SP1 / 2008 R2 SP1 (x64)
1300431	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 3.5.1 - Windows 7 Gold (KB2742598)
1300433	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 3.5.1 - Windows 7 Gold (KB2756920)
1300435	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 3.5.1 - Windows 7 SP1 (KB2742599)
1300439	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 3.5.1 - Windows 7 Gold / Windows Server 2008 R2 (KB2742598) (x64)
1300441	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 3.5.1 - Windows 7 Gold / Windows Server 2008 R2 (KB2756920) (x64)
1300443	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 3.5.1 - Windows 7 SP1 / Windows Server 2008 R2 SP1 (KB2742599) (x64)
1300455	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 3.5 - Windows 8 Gold (KB2742616) (x64)
1300459	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4.5 - Windows 8 Gold (x64)
1300461	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 3.5 - Windows 8 Gold (KB2742616)
1300465	MS13-004: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4.5 - Windows 8 Gold
1300609	MS13-006: Vulnerability in Microsoft Windows Could Allow Security Feature Bypass - Windows 7 Gold
1300611	MS13-006: Vulnerability in Microsoft Windows Could Allow Security Feature Bypass - Windows 7 Gold (x64)
1300701	MS13-007: Vulnerability in Open Data Protocol Could Allow Denial of Service - .NET Framework 3.5 SP1 - Windows XP SP3 / Windows Server 2003 SP2 / Windows Vista SP2 / Windows Server 2008 SP2

1300703	MS13-007: Vulnerability in Open Data Protocol Could Allow Denial of Service - .NET Framework 4 - Windows XP SP3 / Windows Server 2003 SP2 / Windows Vista SP2 / Windows Server 2008 SP2 / Windows 7 Gold/SP1
1300705	MS13-007: Vulnerability in Open Data Protocol Could Allow Denial of Service - .NET Framework 3.5 SP1 - Windows XP SP2 / Windows Server 2003 SP2 / Windows Vista SP2 / Windows Server 2008 SP2 (x64)
1300707	MS13-007: Vulnerability in Open Data Protocol Could Allow Denial of Service - .NET Framework 4 - Windows XP SP2 / 2003 SP2 / Vista SP2 / Server 2008 SP2 / 7 Gold/SP1 / 2008 R2 Gold/SP1 (x64)
1300709	MS13-007: Vulnerability in Open Data Protocol Could Allow Denial of Service - .NET Framework 3.5.1 - Windows 7 Gold
1300711	MS13-007: Vulnerability in Open Data Protocol Could Allow Denial of Service - .NET Framework 3.5.1 - Windows 7 SP1
1300713	MS13-007: Vulnerability in Open Data Protocol Could Allow Denial of Service - .NET Framework 3.5.1 - Windows 7 Gold / Windows Server 2008 R2 (x64)
1300715	MS13-007: Vulnerability in Open Data Protocol Could Allow Denial of Service - .NET Framework 3.5.1 - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)
1300721	MS13-007: Vulnerability in Open Data Protocol Could Allow Denial of Service - .NET Framework 3.5 - Windows 8 Gold (x64)
1300723	MS13-007: Vulnerability in Open Data Protocol Could Allow Denial of Service - .NET Framework 3.5 - Windows 8 Gold
1301103	MS13-011: Vulnerability in Media Decompression Could Allow Remote Code Execution - Quartz.dll (DirectShow) - Windows XP SP2 (x64)
1301104	MS13-011: Vulnerability in Media Decompression Could Allow Remote Code Execution - Quartz.dll (DirectShow) - Windows XP SP2 (x64) - CORRUPT PATCH
1301501	MS13-015: Vulnerability in .NET Framework Could Allow Elevation of Privilege - .NET Framework 2.0 SP2 - Windows XP SP3
1301503	MS13-015: Vulnerability in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4 - Windows XP SP3 / Windows 7 Gold
1301505	MS13-015: Vulnerability in .NET Framework Could Allow Elevation of Privilege - .NET Framework 2.0 SP2 - Windows XP SP2 (x64)
1301507	MS13-015: Vulnerability in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4 - Windows XP SP2 / Windows 7 Gold / Windows Server 2008 R2 Gold (x64)
1301517	MS13-015: Vulnerability in .NET Framework Could Allow Elevation of Privilege - .NET Framework 3.5.1 - Windows 7 Gold
1301519	MS13-015: Vulnerability in .NET Framework Could Allow Elevation of Privilege - .NET Framework 3.5.1 - Windows 7 SP1

1301521	MS13-015: Vulnerability in .NET Framework Could Allow Elevation of Privilege - .NET Framework 3.5.1 - Windows 7 Gold / Windows Server 2008 R2 Gold (x64)
1301523	MS13-015: Vulnerability in .NET Framework Could Allow Elevation of Privilege - .NET Framework 3.5.1 - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)
1301901	MS13-019: Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege - Windows 7 Gold
1302703	MS13-027: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege - Windows XP SP2 (x64)
1302704	MS13-027: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege - Windows XP SP2 (x64) - CORRUPT PATCH
1302709	MS13-027: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege - Windows Vista SP2
1302711	MS13-027: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege - Windows Vista SP2 (x64)
1302717	MS13-027: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege - Windows 7 Gold/SP1
1302719	MS13-027: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege - Windows 7 Gold/SP1 (x64)
1302723	MS13-027: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege - Windows 8 Gold
1302725	MS13-027: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege - Windows 8 Gold (x64)
1302841	MS13-028: Cumulative Security Update for Internet Explorer - IE 8 - Windows 7 Gold
1302843	MS13-028: Cumulative Security Update for Internet Explorer - IE 8 - Windows 7 Gold(x64)
1302845	MS13-028: Cumulative Security Update for Internet Explorer - IE 8 - Windows Server 2008 R2 Gold (x64)
1302855	MS13-028: Cumulative Security Update for Internet Explorer - IE 9 - Windows 7 Gold
1302857	MS13-028: Cumulative Security Update for Internet Explorer - IE 9 - Windows 7 Gold (x64)
1302859	MS13-028: Cumulative Security Update for Internet Explorer - IE 9 - Windows Server 2008 R2 Gold (x64)
1302905	MS13-029: Vulnerability in Remote Desktop Client Could Allow Remote Code Execution - Remote Desktop Connection 6.1 Client - Windows XP SP2 (x64)
1302923	MS13-029: Vulnerability in Remote Desktop Client Could Allow Remote Code Execution - Remote Desktop Connection 7.0/7.1 Client - Windows 7 Gold

1302925	MS13-029: Vulnerability in Remote Desktop Client Could Allow Remote Code Execution - Remote Desktop Connection 7.0/7.1 Client - Windows 7 Gold (x64)
1303103	MS13-031: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege - Windows XP SP2 (x64)
1303104	MS13-031: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege - Windows XP SP2 (x64) - CORRUPT PATCH
1303117	MS13-031: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege - Windows 7 Gold
1303119	MS13-031: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege - Windows 7 Gold (x64)
1303221	MS13-032: Vulnerability in Active Directory Could Lead to Denial of Service - Active Directory Lightweight Directory Service (AD LDS) - Windows 7 Gold
1303223	MS13-032: Vulnerability in Active Directory Could Lead to Denial of Service - Active Directory Lightweight Directory Service (AD LDS) - Windows 7 Gold (x64)
1303227	MS13-032: Vulnerability in Active Directory Could Lead to Denial of Service - Active Directory Lightweight Directory Service (AD LDS) - Windows 8 Gold
1303229	MS13-032: Vulnerability in Active Directory Could Lead to Denial of Service - Active Directory Lightweight Directory Service (AD LDS) - Windows 8 Gold (x64)
1303303	MS13-033: Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege - Windows XP SP2 (x64)
1303304	MS13-033: Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege - Windows XP SP2 (x64) - CORRUPT PATCH
1303309	MS13-033: Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege - Windows Vista SP2
1303311	MS13-033: Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege - Windows Vista SP2 (x64)
1303401	MS13-034: Vulnerability in Microsoft Antimalware Client Could Allow Elevation of Privilege - Windows 8 Gold
1303403	MS13-034: Vulnerability in Microsoft Antimalware Client Could Allow Elevation of Privilege - Windows 8 Gold (x64)
1303644	MS13-036: Vulnerabilities in Kernel-Mode Driver Could Allow Elevation Of Privilege - Windows Vista SP2 (KB2823324) - Uninstall
1303648	MS13-036: Vulnerabilities in Kernel-Mode Driver Could Allow Elevation Of Privilege - Windows 7 Gold/SP1 (KB2823324) - Uninstall
1303650	MS13-036: Vulnerabilities in Kernel-Mode Driver Could Allow Elevation Of Privilege - Windows Vista SP2 (x64) (KB2823324) - Uninstall

1303654	MS13-036: Vulnerabilities in Kernel-Mode Driver Could Allow Elevation Of Privilege - Windows 7 Gold/SP1 (x64) (KB2823324) - Uninstall
1303657	MS13-036: Vulnerabilities in Kernel-Mode Driver Could Allow Elevation Of Privilege - Windows Vista SP2 (KB2840149)
1303659	MS13-036: Vulnerabilities in Kernel-Mode Driver Could Allow Elevation Of Privilege - Windows Vista SP2 (x64) (KB2840149)
1303665	MS13-036: Vulnerabilities in Kernel-Mode Driver Could Allow Elevation Of Privilege - Windows 7 Gold (KB2840149)
1303667	MS13-036: Vulnerabilities in Kernel-Mode Driver Could Allow Elevation Of Privilege - Windows 7 Gold (x64) (KB2840149)
1305015	MS13-050: Vulnerability in Windows Print Spooler Components Could Allow Elevation of Privilege - Windows 8 Gold
1305017	MS13-050: Vulnerability in Windows Print Spooler Components Could Allow Elevation of Privilege - Windows 8 Gold (x64)
1305203	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution - .NET Framework 1.1 SP1 - Windows XP / 2003 SP2 (x64) / Vista SP2 / 2008 SP2
1305207	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution - .NET Framework 2.0 SP2 - Windows XP SP3 / Windows Server 2003 SP2 (KB2844285) (V2.0)
1305209	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution - .NET Framework 3.0 SP2 - Windows XP SP3
1305211	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution - .NET Framework 3.5 SP1 - Windows XP SP3 / 2003 SP2 / Vista SP2 / 2008 SP2
1305217	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution - .NET Framework 4 - Windows XP SP3 / 2003 SP2 / Vista SP2 / 2008 SP2 / 7 SP1 (KB2840628) (V2.0)
1305221	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution - .NET Framework 2.0 SP2 - Windows XP SP2 / 2003 SP2 (x64) (KB2844285) (V2.0)
1305223	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution - .NET Framework 3.0 SP2 - Windows XP SP2 (x64)
1305229	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution - .NET Framework 4 - Windows XP SP2 / 2003 SP2 / Vista SP2 / 2008 SP2 / 7 SP1 / 2008 R2 SP1 (x64) (V2.0)
1305233	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution - .NET Framework 3.5 SP1 - Windows XP SP2 / Server 2003 SP2 / Vista SP2 / 2008 SP2 (x64)
1305245	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution - .NET Framework 4.5 - Windows Vista SP2 / 2008 SP2 / 7 SP1 (KB2840642) (V2.0)

1305257	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution - .NET Framework 4.5 - Windows Vista SP2 / Server 2008 SP2 / 7 SP1 / Server 2008 R2 SP1 (x64) (V2.0)
1305263	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution - .NET Framework 3.5.1 - Windows 7 SP1 (KB2840631)
1305271	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution - .NET Framework 3.5.1 - Windows 7 SP1 / 2008 R2 SP1 (x64) (KB2840631)
1305279	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution - .NET Framework 3.5 - Windows 8 Gold (KB2840633)
1305285	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution - .NET Framework 4.5 - Windows 8 Gold (KB2840632) (V2.0)
1305291	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution - .NET Framework 3.5 - Windows 8 / Server 2012 (x64)(KB2840633)
1305297	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution - .NET Framework 4.5 - Windows 8 / Server 2012 (x64) (KB2840632) (V2.0)
1305405	MS13-054: Vulnerability in GDI+ Could Allow Remote Code Execution - KB2834886 - Windows XP SP2 (x64)
1305406	MS13-054: Vulnerability in GDI+ Could Allow Remote Code Execution - KB2834886 - Windows XP SP2 (x64) - CORRUPT PATCH
1305713	MS13-057: Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 - Windows XP SP2 (x64) (V3.0)
1305714	MS13-057: Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 - Windows XP SP2 (x64) (V3.0) - CORRUPT PATCH
1305715	MS13-057: Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 x64 - Windows XP SP2 / Windows Server 2003 SP2 (x64) (V3.0)
1305716	MS13-057: Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution - Windows Media Format Runtime 9.5 x64 - Windows XP SP2 / Windows Server 2003 SP2 (x64) (V3.0) - CORRUPT PATCH
1305717	MS13-057: Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution - Windows Media Format Runtime 11 - Windows XP SP2 / Windows Server 2003 SP2 (x64) (V3.0)

1305718	MS13-057: Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution - Windows Media Format Runtime 11 - Windows XP SP2 / Windows Server 2003 SP2 (x64) (V3.0) - CORRUPT PATCH
1305719	MS13-057: Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution - wmv9vcm.dll (codec) - Windows XP SP2 / Windows Server 2003 SP2 (x64)
1305729	MS13-057: Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution - wmv9vcm.dll (codec) - Windows Vista SP2 / Windows Server 2008 SP2
1305733	MS13-057: Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution - wmv9vcm.dll (codec) - Windows Vista SP2 / Windows Server 2008 SP2 (x64)
1305801	MS13-058: Vulnerability in Windows Defender Could Allow Elevation of Privilege - Windows Defender for Windows 7 SP1
1305803	MS13-058: Vulnerability in Windows Defender Could Allow Elevation of Privilege - Windows Defender for Windows 7 SP1 (x64)
1306003	MS13-060: Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution - Windows XP SP2 (x64)
1306004	MS13-060: Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1307003	MS13-070: Vulnerability in OLE Could Allow Remote Code Execution - Windows XP SP2 (x64)
1307004	MS13-070: Vulnerability in OLE Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1307103	MS13-071: Vulnerability in Windows Theme File Could Allow Remote Code Execution - Windows XP SP2 (x64)
1307104	MS13-071: Vulnerability in Windows Theme File Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1307109	MS13-071: Vulnerability in Windows Theme File Could Allow Remote Code Execution - Windows Vista SP2
1307111	MS13-071: Vulnerability in Windows Theme File Could Allow Remote Code Execution - Windows Vista SP2 (x64)
1307603	MS13-076: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege - Windows XP SP2 (x64)
1307604	MS13-076: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege - Windows XP SP2 (x64) - CORRUPT PATCH
1307901	MS13-079: Vulnerability in Active Directory Could Allow Denial of Service - Active Directory Lightweight Directory Service (AD LDS) - Windows Vista SP2
1307903	MS13-079: Vulnerability in Active Directory Could Allow Denial of Service - Active Directory Lightweight Directory Service (AD LDS) - Windows Vista SP2 (x64)

1307909	MS13-079: Vulnerability in Active Directory Could Allow Denial of Service - Active Directory Lightweight Directory Service (AD LDS) - Windows 7 SP1
1307911	MS13-079: Vulnerability in Active Directory Could Allow Denial of Service - Active Directory Lightweight Directory Service (AD LDS) - Windows 7 SP1 (x64)
1307915	MS13-079: Vulnerability in Active Directory Could Allow Denial of Service - Active Directory Lightweight Directory Service (AD LDS) - Windows 8 Gold
1307917	MS13-079: Vulnerability in Active Directory Could Allow Denial of Service - Active Directory Lightweight Directory Service (AD LDS) - Windows 8 Gold (x64)
1308113	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2847311 - Windows XP SP2 (x64)
1308114	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2847311 - Windows XP SP2 (x64) - CORRUPT PATCH
1308115	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2862330 - Windows XP SP2 (x64)
1308116	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2862330 - Windows XP SP2 (x64) - CORRUPT PATCH
1308117	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2862335 - Windows XP SP2 (x64)
1308118	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2862335 - Windows XP SP2 (x64) - CORRUPT PATCH
1308119	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2868038 - Windows XP SP2 (x64)
1308120	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2868038 - Windows XP SP2 (x64) - CORRUPT PATCH
1308123	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2884256 - Windows XP SP2 (x64)
1308124	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2884256 - Windows XP SP2 (x64) - CORRUPT PATCH
1308153	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2862330 - Windows Vista SP2
1308155	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2862335 - Windows Vista SP2
1308157	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2864202 - Windows Vista SP2

1308159	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2868038 - Windows Vista SP2
1308165	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2884256 - Windows Vista SP2
1308171	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2862330 - Windows Vista SP2 (x64)
1308173	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2862335 - Windows Vista SP2 (x64)
1308175	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2864202 - Windows Vista SP2 (x64)
1308177	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2868038 - Windows Vista SP2 (x64)
1308183	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2884256 - Windows Vista SP2 (x64)
1308201	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 2.0 SP2 - KB2863239 - Windows XP SP3
1308203	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 3.0 SP2 - KB2861189 - Windows XP SP3
1308205	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 3.5 SP1 - KB2861697 - Windows XP SP3 / Windows Server 2003 SP2 / Windows Vista SP2 / Windows Server 2008 SP2
1308207	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4 - KB2858302 - Windows XP SP3 / Windows Server 2003 SP2 / Windows Vista SP2 / Windows Server 2008 SP2 / Windows 7 SP1
1308209	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4 - KB2861188 - Windows XP SP3 / Windows Server 2003 SP2 / Windows Vista SP2 / Windows Server 2008 SP2
1308211	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 2.0 SP2 - KB2863239 - Windows XP SP2 (x64)
1308213	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 3.0 SP2 - KB2861189 - Windows XP SP2 (x64)
1308215	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 3.5 SP1 - KB2861697 - Windows XP SP2 / Windows Server 2003 SP2 / Windows Vista SP2 / Windows Server 2008 SP2 (x64)
1308217	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4 - KB2858302 - Windows XP SP2 / Windows Server 2003 SP2 / Windows Vista SP2 / Windows Server 2008 SP2 / Windows 7 SP1 (x64)

1308219	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4 - KB2861188 - Windows XP SP2 / Windows Server 2003 SP2 / Windows Vista SP2 / Windows Server 2008 SP2 (x64)
1308225	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4.5 - KB2861193 - Windows Vista SP2 / Windows Server 2008 SP2
1308227	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4.5 - KB2861208 - Windows Vista SP2 / Windows Server 2008 SP2 / Windows 7 SP1
1308233	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4.5 - KB2861193 - Windows Vista SP2 / Windows Server 2008 SP2 (x64)
1308235	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4.5 - KB2861208 - Windows Vista SP2 / Windows Server 2008 SP2 / Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)
1308239	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 3.5.1 - KB2861698 - Windows 7 SP1
1308245	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 3.5.1 - KB2861698 - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)
1308251	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 3.5 - KB2861704 - Windows 8 Gold
1308255	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4.5 - KB2861702 - Windows 8 Gold
1308259	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 3.5 - KB2861704 - Windows 8 / Windows Server 2012 / Windows Server 2012 Gold (x64)
1308263	MS13-082: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - .NET Framework 4.5 - KB2861702 - Windows 8 Gold / Windows Server 2012 Gold (x64)
1308301	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution - Windows XP SP2 (x64)
1308302	MS13-083: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1308903	MS13-089: Vulnerability in Windows Graphics Device Interface Could Allow Remote Code Execution - Windows XP SP2 (x64)
1308904	MS13-089: Vulnerability in Windows Graphics Device Interface Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1309001	MS13-090: Cumulative Security Update of ActiveX Kill Bits - Windows XP SP3

1309003	MS13-090: Cumulative Security Update of ActiveX Kill Bits - Windows XP SP2 (x64)
1309037	MS13-090: Cumulative Security Update of ActiveX Kill Bits - Windows 8 Gold - KB2900986
1309049	MS13-090: Cumulative Security Update of ActiveX Kill Bits - Windows Vista SP2 - KB2900986
1309051	MS13-090: Cumulative Security Update of ActiveX Kill Bits - Windows 8 Gold - KB2900986 (x64)
1309061	MS13-090: Cumulative Security Update of ActiveX Kill Bits - Windows 7 SP1 - KB2900986
1309065	MS13-090: Cumulative Security Update of ActiveX Kill Bits - Windows 7 SP1 - KB2900986 (x64)
1309067	MS13-090: Cumulative Security Update of ActiveX Kill Bits - Windows Vista SP2 - KB2900986 (x64)
1309201	MS13-092: Vulnerability in Hyper-V Could Allow Elevation of Privilege - Windows 8 Gold (x64)
1309301	MS13-093: Vulnerability in Windows Ancillary Function Driver Could Allow Information Disclosure - Windows XP SP2 (x64)
1309302	MS13-093: Vulnerability in Windows Ancillary Function Driver Could Allow Information Disclosure - Windows XP SP2 (x64) - CORRUPT PATCH
1309503	MS13-095: Vulnerability in Digital Signatures Could Allow Denial of Service - Windows XP SP2 (x64)
1309504	MS13-095: Vulnerability in Digital Signatures Could Allow Denial of Service - Windows XP SP2 (x64) - CORRUPT PATCH
1309509	MS13-095: Vulnerability in Digital Signatures Could Allow Denial of Service - Windows Vista SP2
1309511	MS13-095: Vulnerability in Digital Signatures Could Allow Denial of Service - Windows Vista SP2 (x64)
1309523	MS13-095: Vulnerability in Digital Signatures Could Allow Denial of Service - Windows 8 Gold
1309525	MS13-095: Vulnerability in Digital Signatures Could Allow Denial of Service - Windows 8 Gold (x64)
1309527	MS13-095: Vulnerability in Digital Signatures Could Allow Denial of Service - Windows 8.1 Gold
1309529	MS13-095: Vulnerability in Digital Signatures Could Allow Denial of Service - Windows 8.1 Gold (x64)
1309803	MS13-098: Vulnerability in Windows Could Allow Remote Code Execution - Windows XP SP2 (x64)
1309804	MS13-098: Vulnerability in Windows Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1309809	MS13-098: Vulnerability in Windows Could Allow Remote Code Execution - Windows Vista SP2

1309811	MS13-098: Vulnerability in Windows Could Allow Remote Code Execution - Windows Vista SP2 (x64)
1309817	MS13-098: Vulnerability in Windows Could Allow Remote Code Execution - Windows 7 SP1
1309819	MS13-098: Vulnerability in Windows Could Allow Remote Code Execution - Windows 7 SP1 (x64)
1309823	MS13-098: Vulnerability in Windows Could Allow Remote Code Execution - Windows 8 Gold
1309825	MS13-098: Vulnerability in Windows Could Allow Remote Code Execution - Windows 8 Gold (x64)
1309827	MS13-098: Vulnerability in Windows Could Allow Remote Code Execution - Windows 8.1 Gold
1309829	MS13-098: Vulnerability in Windows Could Allow Remote Code Execution - Windows 8.1 Gold (x64)
1309903	MS13-099: Vulnerability in Microsoft Scripting Runtime Object Library Could Allow Remote Code Execution - Windows Script 5.6 - Windows XP SP2 (x64)
1309904	MS13-099: Vulnerability in Microsoft Scripting Runtime Object Library Could Allow Remote Code Execution - Windows Script 5.6 - Windows XP SP2 (x64) - CORRUPT PATCH
1309905	MS13-099: Vulnerability in Microsoft Scripting Runtime Object Library Could Allow Remote Code Execution - Windows Script 5.7 - Windows XP SP2 (x64)
1309906	MS13-099: Vulnerability in Microsoft Scripting Runtime Object Library Could Allow Remote Code Execution - Windows Script 5.7 - Windows XP SP2 (x64) - CORRUPT PATCH
1309915	MS13-099: Vulnerability in Microsoft Scripting Runtime Object Library Could Allow Remote Code Execution - Windows Script 5.7 - Windows Vista SP2
1309917	MS13-099: Vulnerability in Microsoft Scripting Runtime Object Library Could Allow Remote Code Execution - Windows Script 5.7 - Windows Vista SP2 (x64)
1309929	MS13-099: Vulnerability in Microsoft Scripting Runtime Object Library Could Allow Remote Code Execution - Windows Script 5.8 - Windows 8 Gold
1309931	MS13-099: Vulnerability in Microsoft Scripting Runtime Object Library Could Allow Remote Code Execution - Windows Script 5.8 - Windows 8 Gold (x64)
1309933	MS13-099: Vulnerability in Microsoft Scripting Runtime Object Library Could Allow Remote Code Execution - Windows Script 5.8 - Windows 8.1 Gold
1309935	MS13-099: Vulnerability in Microsoft Scripting Runtime Object Library Could Allow Remote Code Execution - Windows Script 5.8 - Windows 8.1 Gold (x64)

1310203	MS13-102: Vulnerability in LRPC Client Could Allow Elevation of Privilege - Windows XP SP2 (x64)
1310204	MS13-102: Vulnerability in LRPC Client Could Allow Elevation of Privilege - Windows XP SP2 (x64) - CORRUPT PATCH
1400203	MS14-002: Vulnerability in Windows Kernel Could Allow Elevation of Privilege - Windows XP SP2 (x64)
1400204	MS14-002: Vulnerability in Windows Kernel Could Allow Elevation of Privilege - Windows XP SP2 (x64) - CORRUPT PATCH
1400503	MS14-005: Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure - XML Core Services 3.0 - Windows XP SP2 (x64)
1400504	MS14-005: Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure - XML Core Services 3.0 - Windows XP SP2 (x64) - CORRUPT PATCH
1400701	MS14-007: Vulnerability in Direct2D Could Allow Remote Code Execution - Windows 7 SP1
1400703	MS14-007: Vulnerability in Direct2D Could Allow Remote Code Execution - Windows 7 SP1 (x64)
1400707	MS14-007: Vulnerability in Direct2D Could Allow Remote Code Execution - Windows 8 Gold
1400709	MS14-007: Vulnerability in Direct2D Could Allow Remote Code Execution - Windows 8 Gold (x64)
1400711	MS14-007: Vulnerability in Direct2D Could Allow Remote Code Execution - Windows 8.1 Gold
1400713	MS14-007: Vulnerability in Direct2D Could Allow Remote Code Execution - Windows 8.1 Gold (x64)
1400927	MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 2.0 SP2 - KB2911502 - Windows Vista SP2 / Windows Server 2008 SP2
1400929	MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4.5 - KB2901118 - Windows Vista SP2 / Windows Server 2008 SP2 / Windows 7 SP1
1400931	MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4.5 - KB2898864 - Windows Vista SP2 / Windows Server 2008 SP2 / Windows 7 SP1
1400935	MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4.5.1 - KB2898869 - Windows Vista SP2 / Windows Server 2008 SP2 / Windows 7 SP1
1400941	MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 2.0 SP2 - KB2911502 - Windows Vista SP2 / Windows Server 2008 SP2 (x64)
1400943	MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4.5 - KB2901118 - Windows Vista SP2 / Windows Server 2008 SP2 / Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)

1400945	MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4.5 - KB2898864 - Windows Vista SP2 / Windows Server 2008 SP2 / Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)
1400949	MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4.5.1 - KB2898869 - Windows Vista SP2 / Server 2008 SP2 / 7 SP1 / Server 2008 R2 SP1 (x64)
1400955	MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 3.5.1 - KB2911501 - Windows 7 SP1
1400961	MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 3.5.1 - KB2911501 - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)
1400973	MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4.5.1 - KB2898870 - Windows 8 Gold
1400985	MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4.5.1 - KB2898870 - Windows 8 / Windows Server 2012 Gold (x64)
1400993	MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4.5.1 - KB2898871 - Windows 8.1 Gold
1401101	MS14-011: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution - VBScript 5.6 - Windows XP SP2 (x64)
1401102	MS14-011: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution - VBScript 5.6 - Windows XP SP2 (x64) - CORRUPT PATCH
1401109	MS14-011: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution - VBScript 5.7 - Windows XP SP2 (x64)
1401110	MS14-011: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution - VBScript 5.7 - Windows XP SP2 (x64) - CORRUPT PATCH
1401125	MS14-011: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution - VBScript 5.8 - IE8 - Windows XP SP2 (x64)
1401126	MS14-011: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution - VBScript 5.8 - IE8 - Windows XP SP2 (x64) - CORRUPT PATCH
1401303	MS14-013: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution - Windows XP SP2 (x64)
1401304	MS14-013: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1401503	MS14-015: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege - Windows XP SP2 (x64)
1401504	MS14-015: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege - Windows XP SP2 (x64) - CORRUPT PATCH
1401603	MS14-016: Vulnerability in Security Account Manager Remote (SAMR) Protocol Could Allow Security Feature Bypass - Windows XP SP2 (x64)

1401604	MS14-016: Vulnerability in Security Account Manager Remote (SAMR) Protocol Could Allow Security Feature Bypass - Windows XP SP2 (x64) - CORRUPT PATCH
1401613	MS14-016: Vulnerability in Security Account Manager Remote (SAMR) Protocol Could Allow Security Feature Bypass - Windows Vista SP2
1401615	MS14-016: Vulnerability in Security Account Manager Remote (SAMR) Protocol Could Allow Security Feature Bypass - Windows Vista SP2 (x64)
1401801	MS14-018: Cumulative Security Update for Internet Explorer - IE 6 - Windows XP SP3
1401802	MS14-018: Cumulative Security Update for Internet Explorer - IE 6 - Windows XP SP3 - CORRUPT PATCH
1401803	MS14-018: Cumulative Security Update for Internet Explorer - IE 6 - Windows XP SP2 (x64)
1401804	MS14-018: Cumulative Security Update for Internet Explorer - IE 6 - Windows XP SP2 (x64) - CORRUPT PATCH
1401809	MS14-018: Cumulative Security Update for Internet Explorer - IE 7 - Windows XP SP3
1401810	MS14-018: Cumulative Security Update for Internet Explorer - IE 7 - Windows XP SP3 - CORRUPT PATCH
1401811	MS14-018: Cumulative Security Update for Internet Explorer - IE 7 - Windows XP SP2 (x64)
1401812	MS14-018: Cumulative Security Update for Internet Explorer - IE 7 - Windows XP SP2 (x64) - CORRUPT PATCH
1401825	MS14-018: Cumulative Security Update for Internet Explorer - IE 8 - Windows XP SP3
1401826	MS14-018: Cumulative Security Update for Internet Explorer - IE 8 - Windows XP SP3 - CORRUPT PATCH
1401827	MS14-018: Cumulative Security Update for Internet Explorer - IE 8 - Windows XP SP2 (x64)
1401828	MS14-018: Cumulative Security Update for Internet Explorer - IE 8 - Windows XP SP2 (x64) - CORRUPT PATCH
1401903	MS14-019: Vulnerability in Windows File Handling Component Could Allow Remote Code Execution - Windows XP SP2 (x64)
1401904	MS14-019: Vulnerability in Windows File Handling Component Could Allow Remote Code Execution - Windows XP SP2 (x64) - CORRUPT PATCH
1401923	MS14-019: Vulnerability in Windows File Handling Component Could Allow Remote Code Execution - Windows 8 Gold
1401925	MS14-019: Vulnerability in Windows File Handling Component Could Allow Remote Code Execution - Windows 8 Gold (x64)
1401927	MS14-019: Vulnerability in Windows File Handling Component Could Allow Remote Code Execution - Windows 8.1 Gold

1401929	MS14-019: Vulnerability in Windows File Handling Component Could Allow Remote Code Execution - Windows 8.1 Gold (x64)
1402109	MS14-021: Security Update for Internet Explorer - IE 6 - Windows XP SP3
1402110	MS14-021: Security Update for Internet Explorer - IE 6 - Windows XP SP3 - CORRUPT PATCH
1402111	MS14-021: Security Update for Internet Explorer - IE 6 - Windows XP SP2 (x64)
1402112	MS14-021: Security Update for Internet Explorer - IE 6 - Windows XP SP2 (x64) - CORRUPT PATCH
1402117	MS14-021: Security Update for Internet Explorer - IE 7 - Windows XP SP3
1402118	MS14-021: Security Update for Internet Explorer - IE 7 - Windows XP SP3 - CORRUPT PATCH
1402119	MS14-021: Security Update for Internet Explorer - IE 7 - Windows XP SP2 (x64)
1402120	MS14-021: Security Update for Internet Explorer - IE 7 - Windows XP SP2 (x64) - CORRUPT PATCH
1402133	MS14-021: Security Update for Internet Explorer - IE 8 - Windows XP SP3
1402134	MS14-021: Security Update for Internet Explorer - IE 8 - Windows XP SP3 - CORRUPT PATCH
1402135	MS14-021: Security Update for Internet Explorer - IE 8 - Windows XP SP2 (x64)
1402136	MS14-021: Security Update for Internet Explorer - IE 8 - Windows XP SP2 (x64) - CORRUPT PATCH
1402503	MS14-025: Vulnerability in Group Policy Preferences Could Allow Elevation of Privilege - Windows 8.1 Gold - Remote Server Administration Tools - KB2928120 (x64)
1402507	MS14-025: Vulnerability in Group Policy Preferences Could Allow Elevation of Privilege - Windows 8.1 Gold - Remote Server Administration Tools - KB2961899
1402511	MS14-025: Vulnerability in Group Policy Preferences Could Allow Elevation of Privilege - Windows 7 SP1 - Remote Server Administration Tools - KB2928120 (x64)
1402513	MS14-025: Vulnerability in Group Policy Preferences Could Allow Elevation of Privilege - Windows 8 Gold - Remote Server Administration Tools - KB2928120
1402515	MS14-025: Vulnerability in Group Policy Preferences Could Allow Elevation of Privilege - Windows 8 Gold - Remote Server Administration Tools - KB2928120 (x64)
1402517	MS14-025: Vulnerability in Group Policy Preferences Could Allow Elevation of Privilege - Windows 7 SP1 - Remote Server Administration Tools - KB2928120
1402523	MS14-025: Vulnerability in Group Policy Preferences Could Allow Elevation of Privilege - Windows 8.1 Gold - Remote Server Administration Tools - KB2928120

1402525	MS14-025: Vulnerability in Group Policy Preferences Could Allow Elevation of Privilege - Windows 8.1 Gold - Remote Server Administration Tools - KB2961899 (x64)
1402529	MS14-025: Vulnerability in Group Policy Preferences Could Allow Elevation of Privilege - Windows Vista SP2 - Remote Server Administration Tools - KB2928120
1402531	MS14-025: Vulnerability in Group Policy Preferences Could Allow Elevation of Privilege - Windows Vista SP2 - Remote Server Administration Tools - KB2928120 (x64)
1402607	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege - Windows 7 SP1 - .NET Framework 3.5.1 - KB2931356
1402613	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB2931354
1402629	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB2931354 (x64)
1402633	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege - Windows Server 2008 R2 SP1 / Windows 7 SP1 - .NET Framework 3.5.1 - KB2931356 (x64)
1403101	MS14-031: Vulnerability in TCP Protocol Could Allow Denial of Service - Windows 8 Gold - KB2957189
1403113	MS14-031: Vulnerability in TCP Protocol Could Allow Denial of Service - Windows 8 Gold - KB2957189 (x64)
1403119	MS14-031: Vulnerability in TCP Protocol Could Allow Denial of Service - Windows Vista SP2 - KB2957189
1403125	MS14-031: Vulnerability in TCP Protocol Could Allow Denial of Service - Windows Vista SP2 - KB2957189 (x64)
1403601	MS14-036: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows Vista SP2 - KB2957509 (x64)
1403645	MS14-036: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows Vista SP2 - KB2957509
1403901	MS14-039: Vulnerability in On-Screen Keyboard Could Allow Elevation of Privilege - Windows 7 SP1 - KB2973201 (x64)
1403905	MS14-039: Vulnerability in On-Screen Keyboard Could Allow Elevation of Privilege - Windows 8.1 Gold - KB2973201 (x64)
1403907	MS14-039: Vulnerability in On-Screen Keyboard Could Allow Elevation of Privilege - Windows Vista SP2 - KB2973201 (x64)
1403909	MS14-039: Vulnerability in On-Screen Keyboard Could Allow Elevation of Privilege - Windows 8 Gold - KB2973201 (x64)
1403913	MS14-039: Vulnerability in On-Screen Keyboard Could Allow Elevation of Privilege - Windows 8 Gold - KB2973201

1403917	MS14-039: Vulnerability in On-Screen Keyboard Could Allow Elevation of Privilege - Windows Vista SP2 - KB2973201
1403921	MS14-039: Vulnerability in On-Screen Keyboard Could Allow Elevation of Privilege - Windows 8.1 Gold - KB2973201
1403923	MS14-039: Vulnerability in On-Screen Keyboard Could Allow Elevation of Privilege - Windows 7 SP1 - KB2973201
1404301	MS14-043: Vulnerability in Windows Media Center Could Allow Remote Code Execution - Windows Vista SP2 - Windows Media Center TV Pack - KB2978742 (x64)
1404303	MS14-043: Vulnerability in Windows Media Center Could Allow Remote Code Execution - Windows Vista SP2 - Windows Media Center TV Pack - KB2978742
1404305	MS14-043: Vulnerability in Windows Media Center Could Allow Remote Code Execution - Windows 8 Gold - Windows Media Center - KB2978742 (x64)
1404307	MS14-043: Vulnerability in Windows Media Center Could Allow Remote Code Execution - Windows 7 SP1 - KB2978742 (x64)
1404309	MS14-043: Vulnerability in Windows Media Center Could Allow Remote Code Execution - Windows 8.1 Gold - Windows Media Center - KB2978742 (x64)
1404311	MS14-043: Vulnerability in Windows Media Center Could Allow Remote Code Execution - Windows 8.1 Gold - Windows Media Center - KB2978742
1404313	MS14-043: Vulnerability in Windows Media Center Could Allow Remote Code Execution - Windows 8 Gold - Windows Media Center - KB2978742
1404315	MS14-043: Vulnerability in Windows Media Center Could Allow Remote Code Execution - Windows 7 SP1 - KB2978742
1404527	MS14-045: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege - Windows 8 Gold - KB2976897
1404535	MS14-045: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege - Windows 8 Gold - KB2976897 (x64)
1404551	MS14-045: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege - Windows 8.1 Gold - KB2976897
1404553	MS14-045: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege - Windows 8.1 Gold - KB2976897 (x64)
1404563	MS14-045: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege - Windows 8 Gold - KB2993651
1404573	MS14-045: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege - Windows Vista SP2 - KB2993651
1404575	MS14-045: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege - Windows 8 Gold - KB2993651 (x64)

1404577	MS14-045: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege - Windows Vista SP2 - KB2993651 (x64)
1404601	MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass - Windows 8 Gold - .NET Framework 3.5 - KB2966827
1404603	MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass - Windows 8.1 Gold - .NET Framework 3.5 - KB2966828
1404605	MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB2937608 (x64)
1404607	MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 3.5 - KB2966828 (x64)
1404609	MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB2937608
1404611	MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass - Windows 8 Gold - .NET Framework 3.5 - KB2966825
1404613	MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 3.0 SP2 - KB2943344 (x64)
1404615	MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 3.0 SP2 - KB2943344
1404617	MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass - Windows 7 SP1 - .NET Framework 3.5.1 - KB2937610
1404619	MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass - Windows 7 SP1 - .NET Framework 3.5.1 - KB2943357
1404621	MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass - Windows Server 2008 R2 SP1 / Windows 7 SP1 - .NET Framework 3.5.1 - KB2943357 (x64)
1404623	MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass - Windows Server 2008 R2 SP1 / Windows 7 SP1 - .NET Framework 3.5.1 - KB2937610 (x64)
1404625	MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 3.5 - KB2966826 (x64)
1404627	MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 3.5 - KB2966825 (x64)
1404629	MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 3.5 - KB2966827 (x64)
1404631	MS14-046: Vulnerability in .NET Framework Could Allow Security Feature Bypass - Windows 8.1 Gold - .NET Framework 3.5 - KB2966826

1405301	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows 8 Gold - .NET Framework 3.5 - KB2972212
1405303	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows 8 Gold - .NET Framework 3.5 - KB2973113
1405307	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows 8.1 Gold - .NET Framework 3.5 - KB2972213
1405309	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB2974268
1405313	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 / Windows Server 2003 SP2 - .NET Framework 4 - KB2972215 (x64)
1405319	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 3.0 SP2 - KB2974269
1405321	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 3.5 - KB2972213 (x64)
1405323	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows 7 SP1 - .NET Framework 3.5.1 - KB2972211
1405327	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 / Windows Server 2003 SP2 - .NET Framework 4 - KB2972215
1405331	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows 8.1 Gold - .NET Framework 3.5 - KB2973114
1405335	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows Server 2008 R2 SP1 / Windows 7 SP1 - .NET Framework 3.5.1 - KB2972211 (x64)
1405337	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5/4.5.1/4.5.2 - KB2972216
1405339	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 3.5 - KB2973114 (x64)
1405341	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 3.5 - KB2973113 (x64)
1405345	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 3.5 - KB2972212 (x64)
1405347	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 3.0 SP2 - KB2974269 (x64)

1405349	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows 8 Gold - .NET Framework 4.5/4.5.1/4.5.2 - KB2977766
1405353	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 4.5/4.5.1/4.5.2 - KB2977766 (x64)
1405355	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5/4.5.1/4.5.2 - KB2972216 (x64)
1405357	MS14-053: Vulnerability in .NET Framework Could Allow Denial of Service - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB2974268 (x64)
1405701	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 3.5 - KB2972103 (x64)
1405703	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB2972098 (x64)
1405711	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 / Windows Server 2003 SP2 - .NET Framework 4 - KB2972106
1405713	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 3.5 - KB2968296 (x64)
1405723	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows 8.1 Gold - .NET Framework 3.5 - KB2968296
1405731	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 4.5/4.5.1/4.5.2 - KB2979577 (x64)
1405735	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows 7 SP1 - .NET Framework 3.5.1 - KB2968294
1405737	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB2968292 (x64)
1405739	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows Server 2008 R2 SP1 / Windows 7 SP1 - .NET Framework 3.5.1 - KB2968294 (x64)
1405747	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows 8 Gold - .NET Framework 3.5 - KB2972101(Superseded)
1405749	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB2972098

1405751	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows Server 2003 SP2 - .NET Framework 4 - KB2979575 (x64)
1405757	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows 8.1 Gold - .NET Framework 3.5 - KB2972103
1405759	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB2968292
1405767	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 / Windows Server 2003 SP2 - .NET Framework 4 - KB2972106 (x64)
1405769	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows Server 2008 R2 SP1 / Windows 7 SP1 - .NET Framework 3.5.1 - KB2972100 (x64)
1405771	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows 8 Gold - .NET Framework 4.5/4.5.1/4.5.2 - KB2979577
1405773	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows Server 2003 SP2 - .NET Framework 4 - KB2979575
1405775	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows 7 SP1 - .NET Framework 3.5.1 - KB2972100
1405783	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 3.5 - KB2968295 (x64)
1405785	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution - Windows 8 Gold - .NET Framework 3.5 - KB2968295
1406303	MS14-063: Vulnerability in FAT32 Disk Partition Driver Could Allow Elevation of Privilege - Windows Vista SP2 - KB2998579
1406307	MS14-063: Vulnerability in FAT32 Disk Partition Driver Could Allow Elevation of Privilege - Windows Vista SP2 - KB2998579 (x64)
1406417	MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution - Windows 7 SP1 - KB3010788
1406419	MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution - Windows 8 Gold - KB3006226 (x64)
1406425	MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution - Windows 8 Gold - KB3010788 (x64)
1406427	MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution - Windows 8 Gold - KB3006226
1406431	MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution - Windows 7 SP1 - KB3010788 (x64)
1406437	MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution - Windows 8 Gold - KB3010788

1406439	MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution - Windows Vista SP2 - KB3010788 (x64)
1406441	MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution - Windows 8.1 Gold - KB3010788
1406445	MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution - Windows 8.1 Gold - KB3010788 (x64)
1406451	MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution - Windows Vista SP2 - KB3010788
1406601	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution - Windows 8.1 Gold - KB2992611 (x64)
1406613	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution - Windows 7 SP1 - KB2992611
1406619	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution - Windows 8 Gold - KB2992611
1406623	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution - Windows 8 Gold - KB2992611 (x64)
1406627	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution - Windows 8.1 Gold - KB2992611
1406629	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution - Windows 7 SP1 - KB2992611 (x64)
1406801	MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege - Windows 8 Gold - KB3011780 (x64)
1406803	MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege - Windows 7 SP1 - KB3011780
1406805	MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3011780 (x64)
1406813	MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege - Windows 7 SP1 - KB3011780 (x64)
1406819	MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege - Windows Vista SP2 - KB3011780
1406821	MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3011780
1406823	MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege - Windows Vista SP2 - KB3011780 (x64)
1406829	MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege - Windows 8 Gold - KB3011780
1407105	MS14-071: Vulnerability in Windows Audio Service Could Allow Elevation of Privilege - Windows Vista SP2 - KB3005607 (x64)
1407117	MS14-071: Vulnerability in Windows Audio Service Could Allow Elevation of Privilege - Windows Vista SP2 - KB3005607
1407201	MS14-072: Vulnerability in .NET Framework Could Allow Elevation of Privilege - Windows Vista SP2 - .NET Framework 2.0 SP2 - KB2978116 (x64)

1407203	MS14-072: Vulnerability in .NET Framework Could Allow Elevation of Privilege - Windows Vista SP2 - .NET Framework 4.5/4.5.1/4.5.2 - KB2978128 (x64)
1407207	MS14-072: Vulnerability in .NET Framework Could Allow Elevation of Privilege - Windows Vista SP2 - .NET Framework 4.5/4.5.1/4.5.2 - KB2978128
1407219	MS14-072: Vulnerability in .NET Framework Could Allow Elevation of Privilege - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 4.5.1 - KB2978126 (x64)
1407223	MS14-072: Vulnerability in .NET Framework Could Allow Elevation of Privilege - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 / Windows Server 2003 SP2 - .NET Framework 4 - KB2978125
1407227	MS14-072: Vulnerability in .NET Framework Could Allow Elevation of Privilege - Windows Vista SP2 - .NET Framework 2.0 SP2 - KB2978116
1407229	MS14-072: Vulnerability in .NET Framework Could Allow Elevation of Privilege - Windows 8.1 Gold - .NET Framework 4.5.1 - KB2978126
1407231	MS14-072: Vulnerability in .NET Framework Could Allow Elevation of Privilege - Windows 8 Gold - .NET Framework 3.5 - KB2978121
1407235	MS14-072: Vulnerability in .NET Framework Could Allow Elevation of Privilege - Windows 8 Gold - .NET Framework 3.5 - KB2978121 (x64)
1407237	MS14-072: Vulnerability in .NET Framework Could Allow Elevation of Privilege - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 / Windows Server 2003 SP2 - .NET Framework 4 - KB2978125 (x64)
1407401	MS14-074: Vulnerability in Remote Desktop Protocol Could Allow Security Feature Bypass - Windows 8 Gold - KB3003743
1407403	MS14-074: Vulnerability in Remote Desktop Protocol Could Allow Security Feature Bypass - Windows Vista SP2 - KB3003743 (x64)
1407405	MS14-074: Vulnerability in Remote Desktop Protocol Could Allow Security Feature Bypass - Windows Vista SP2 - KB3003743
1407413	MS14-074: Vulnerability in Remote Desktop Protocol Could Allow Security Feature Bypass - Windows 8 Gold - KB3003743 (x64)
1407601	MS14-076: Vulnerability in Internet Information Services (IIS) Could Allow Security Feature Bypass - Windows 8.1 Gold - IIS 8.5 - KB2982998 (x64)
1407603	MS14-076: Vulnerability in Internet Information Services (IIS) Could Allow Security Feature Bypass - Windows 8.1 Gold - IIS 8.5 - KB2982998
1407605	MS14-076: Vulnerability in Internet Information Services (IIS) Could Allow Security Feature Bypass - Windows 8 Gold - IIS 8.0 - KB2982998 (x64)
1407611	MS14-076: Vulnerability in Internet Information Services (IIS) Could Allow Security Feature Bypass - Windows 8 Gold - IIS 8.0 - KB2982998
1407801	MS14-078: Vulnerability in IME (Japanese) Could Allow Elevation of Privilege - Windows 7 SP1 - KB2991963

1407805	MS14-078: Vulnerability in IME (Japanese) Could Allow Elevation of Privilege - Windows Vista SP2 - KB2991963 (x64)
1407807	MS14-078: Vulnerability in IME (Japanese) Could Allow Elevation of Privilege - Windows Vista SP2 - KB2991963
1407817	MS14-078: Vulnerability in IME (Japanese) Could Allow Elevation of Privilege - Windows 7 SP1 - KB2991963 (x64)
1500103	MS15-001: Vulnerability in Windows Application Compatibility Cache Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3023266 (x64)
1500117	MS15-001: Vulnerability in Windows Application Compatibility Cache Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3023266
1500201	MS15-002: Vulnerability in Windows Telnet Service Could Allow Remote Code Execution - Windows 8.1 Gold - KB3020393 (x64)
1500203	MS15-002: Vulnerability in Windows Telnet Service Could Allow Remote Code Execution - Windows 8 Gold - KB3020393 (x64)
1500205	MS15-002: Vulnerability in Windows Telnet Service Could Allow Remote Code Execution - Windows 7 SP1 - KB3020393
1500207	MS15-002: Vulnerability in Windows Telnet Service Could Allow Remote Code Execution - Windows Vista SP2 - KB3020393
1500209	MS15-002: Vulnerability in Windows Telnet Service Could Allow Remote Code Execution - Windows 8.1 Gold - KB3020393
1500219	MS15-002: Vulnerability in Windows Telnet Service Could Allow Remote Code Execution - Windows 7 SP1 - KB3020393 (x64)
1500225	MS15-002: Vulnerability in Windows Telnet Service Could Allow Remote Code Execution - Windows 8 Gold - KB3020393
1500229	MS15-002: Vulnerability in Windows Telnet Service Could Allow Remote Code Execution - Windows Vista SP2 - KB3020393 (x64)
1500301	MS15-003: Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege - Windows 7 SP1 - KB3021674
1500309	MS15-003: Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege - Windows 8 Gold - KB3021674
1500313	MS15-003: Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege - Windows Vista SP2 - KB3021674 (x64)
1500317	MS15-003: Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege - Windows Vista SP2 - KB3021674
1500319	MS15-003: Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3021674 (x64)
1500323	MS15-003: Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege - Windows 7 SP1 - KB3021674 (x64)
1500327	MS15-003: Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3021674
1500329	MS15-003: Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege - Windows 8 Gold - KB3021674 (x64)

1500403	MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3019978 (x64)
1500405	MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege - Windows 8 Gold - KB3019978
1500407	MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege - Windows Vista SP2 - KB3023299
1500409	MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege - Windows 7 SP1 - KB3019978
1500411	MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege - Windows 7 SP1 - KB3020387
1500413	MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege - Windows 7 SP1 - KB3020388 (x64)
1500421	MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege - Windows 7 SP1 - KB3019978 (x64)
1500423	MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege - Windows 8 Gold - KB3019978 (x64)
1500425	MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege - Windows 7 SP1 - KB3020387 (x64)
1500427	MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3019978
1500431	MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege - Windows Vista SP2 - KB3023299 (x64)
1500433	MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege - Windows 7 SP1 - KB3020388
1500501	MS15-005: Vulnerability in Network Location Awareness Service Could Allow Security Feature Bypass - Windows Vista SP2 - KB3022777 (x64)
1500513	MS15-005: Vulnerability in Network Location Awareness Service Could Allow Security Feature Bypass - Windows 7 SP1 - KB3022777
1500515	MS15-005: Vulnerability in Network Location Awareness Service Could Allow Security Feature Bypass - Windows 8 Gold - KB3022777
1500519	MS15-005: Vulnerability in Network Location Awareness Service Could Allow Security Feature Bypass - Windows 8 Gold - KB3022777 (x64)
1500521	MS15-005: Vulnerability in Network Location Awareness Service Could Allow Security Feature Bypass - Windows Vista SP2 - KB3022777
1500525	MS15-005: Vulnerability in Network Location Awareness Service Could Allow Security Feature Bypass - Windows 7 SP1 - KB3022777 (x64)
1500601	MS15-006: Vulnerability in Windows Error Reporting Could Allow Security Feature Bypass - Windows 8 Gold - KB3004365 (x64)
1500607	MS15-006: Vulnerability in Windows Error Reporting Could Allow Security Feature Bypass - Windows 8.1 Gold - KB3004365 (V2.0)
1500609	MS15-006: Vulnerability in Windows Error Reporting Could Allow Security Feature Bypass - Windows 8 Gold - KB3004365

1500611	MS15-006: Vulnerability in Windows Error Reporting Could Allow Security Feature Bypass - Windows 8.1 Gold - KB3004365 (x64) (V2.0)
1500807	MS15-008: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege - Windows 8 Gold - KB3019215 (x64)
1500815	MS15-008: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege - Windows 8 Gold - KB3019215
1500922	MS15-009: Security Update for Internet Explorer - Windows Server 2012 R2 Gold - IE11 - KB3023607 (x64)
1500942	MS15-009: Security Update for Internet Explorer - Windows 7 SP1 - IE11 - KB3023607 (x64)
1500944	MS15-009: Security Update for Internet Explorer - Windows Server 2008 R2 SP1 - IE11- KB3023607 (x64)
1500968	MS15-009: Security Update for Internet Explorer - Windows 7 SP1 - IE11 - KB3023607
1500970	MS15-009: Security Update for Internet Explorer - Windows 8.1 Gold - IE11 - KB3023607 (x64)
1501101	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution - Windows 7 SP1 - KB3000483 (x64)
1501103	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution - Windows Vista SP2 - KB3000483
1501105	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution - Windows 8.1 Gold - KB3000483 (x64)
1501107	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution - Windows 8 Gold - KB3000483 (x64)
1501111	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution - Windows 8.1 Gold - KB3000483
1501113	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution - Windows 8 Gold - KB3000483
1501117	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution - Windows Vista SP2 - KB3000483 (x64)
1501119	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution - Windows 7 SP1 - KB3000483
1501401	MS15-014: Vulnerability in Group Policy Could Allow Security Feature Bypass - Windows Vista SP2 - KB3004361 (x64)
1501403	MS15-014: Vulnerability in Group Policy Could Allow Security Feature Bypass - Windows Vista SP2 - KB3004361
1501407	MS15-014: Vulnerability in Group Policy Could Allow Security Feature Bypass - Windows 8 Gold - KB3004361
1501409	MS15-014: Vulnerability in Group Policy Could Allow Security Feature Bypass - Windows 7 SP1 - KB3004361 (x64)
1501411	MS15-014: Vulnerability in Group Policy Could Allow Security Feature Bypass - Windows 7 SP1 - KB3004361

1501419	MS15-014: Vulnerability in Group Policy Could Allow Security Feature Bypass - Windows 8.1 Gold - KB3004361 (x64)
1501421	MS15-014: Vulnerability in Group Policy Could Allow Security Feature Bypass - Windows 8 Gold - KB3004361 (x64)
1501423	MS15-014: Vulnerability in Group Policy Could Allow Security Feature Bypass - Windows 8.1 Gold - KB3004361
1501503	MS15-015: Vulnerability in Microsoft Windows Could Allow Elevation of Privilege - Windows 8 Gold - KB3031432 (x64)
1501509	MS15-015: Vulnerability in Microsoft Windows Could Allow Elevation of Privilege - Windows 7 SP1 - KB3031432 (x64)
1501515	MS15-015: Vulnerability in Microsoft Windows Could Allow Elevation of Privilege - Windows 8 Gold - KB3031432
1501517	MS15-015: Vulnerability in Microsoft Windows Could Allow Elevation of Privilege - Windows 7 SP1 - KB3031432
1501873	MS15-018: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 11 - KB3023607 (x64)
1501875	MS15-018: Cumulative Security Update for Internet Explorer - Windows 7 SP1 - IE 11 - KB3023607
1501877	MS15-018: Cumulative Security Update for Internet Explorer - Windows 8.1 Gold - IE 11 - KB3040335 (x64)
1501879	MS15-018: Cumulative Security Update for Internet Explorer - Windows 8.1 Gold - IE 11 - KB3040335
1501881	MS15-018: Cumulative Security Update for Internet Explorer - Windows Server 2008 R2 SP1 - IE 11 - KB3023607 (x64)
1501883	MS15-018: Cumulative Security Update for Internet Explorer - Windows Server 2012 R2 Gold - IE 11 - KB3040335 (x64)
1502001	MS15-020: Vulnerabilities in Microsoft Windows Could Allow Remote Code Execution - Windows 8 Gold - KB3033889
1502019	MS15-020: Vulnerabilities in Microsoft Windows Could Allow Remote Code Execution - Windows 8 Gold - KB3033889 (x64)
1502409	MS15-024: Vulnerability in PNG Processing Could Allow Information Disclosure - Windows 8 Gold - KB3035132
1502415	MS15-024: Vulnerability in PNG Processing Could Allow Information Disclosure - Windows 8 Gold - KB3035132 (x64)
1502417	MS15-024: Vulnerability in PNG Processing Could Allow Information Disclosure - Windows Vista SP2 - KB3035132
1502429	MS15-024: Vulnerability in PNG Processing Could Allow Information Disclosure - Windows Vista SP2 - KB3035132 (x64)
1502801	MS15-028: Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass - Windows 7 SP1 - KB3030377 (x64)
1502805	MS15-028: Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass - Windows 8.1 Gold - KB3030377 (x64)

1502807	MS15-028: Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass - Windows 8 Gold - KB3030377
1502809	MS15-028: Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass - Windows 8.1 Gold - KB3030377
1502811	MS15-028: Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass - Windows 7 SP1 - KB3030377
1502813	MS15-028: Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass - Windows 8 Gold - KB3030377 (x64)
1502905	MS15-029: Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure - Windows 8.1 Gold - KB3035126 (x64)
1502909	MS15-029: Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure - Windows 7 SP1 - KB3035126
1502911	MS15-029: Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure - Windows 8.1 Gold - KB3035126
1502913	MS15-029: Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure - Windows 8 Gold - KB3035126 (x64)
1502915	MS15-029: Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure - Windows 8 Gold - KB3035126
1502917	MS15-029: Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure - Windows Vista SP2 - KB3035126 (x64)
1502919	MS15-029: Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure - Windows Vista SP2 - KB3035126
1502925	MS15-029: Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure - Windows 7 SP1 - KB3035126 (x64)
1503405	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution - Windows 8 Gold - KB3042553 (x64)
1503407	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution - Windows 8 Gold - KB3042553
1503701	MS15-037: Vulnerability in Windows Task Scheduler Could Allow Elevation of Privilege - Windows 7 SP1 - KB3046269 (x64)
1503705	MS15-037: Vulnerability in Windows Task Scheduler Could Allow Elevation of Privilege - Windows 7 SP1 - KB3046269
1503803	MS15-038: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3045685 (x64)
1503809	MS15-038: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege - Windows 8 Gold - KB3045685
1503813	MS15-038: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3045999 (x64)
1503817	MS15-038: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege - Windows Vista SP2 - KB3045685
1503819	MS15-038: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3045685

1503825	MS15-038: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3045999
1503835	MS15-038: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege - Windows 8 Gold - KB3045685 (x64)
1503837	MS15-038: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege - Windows Vista SP2 - KB3045685 (x64)
1503847	MS15-038: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege - Windows 7 SP1 - KB3045685
1503853	MS15-038: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege - Windows 7 SP1 - KB3045685 (x64)
1504101	MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 / Windows Server 2003 SP2 - .NET Framework 4 - KB3037578 (x64)
1504103	MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure - Windows 8.1 Gold - .NET Framework 4.5.1 - KB3037579
1504105	MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 4.5/4.5.1/4.5.2 - KB3037580 (x64) (V2.0)
1504107	MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 4.5.1 - KB3037579 (x64)
1504109	MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure - Windows Server 2008 R2 SP1 / Windows 7 SP1 - .NET Framework 3.5.1 - KB3037574 (x64)
1504111	MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB3037573 (x64)
1504113	MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure - Windows 8 Gold - .NET Framework 3.5 - KB3037575
1504115	MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5/4.5.1/4.5.2 - KB3037581
1504119	MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure - Windows 7 SP1 - .NET Framework 3.5.1 - KB3037574
1504121	MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 3.5 - KB3037575 (x64)
1504123	MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 / Windows Server 2003 SP2 - .NET Framework 4 - KB3037578

1504125	MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5/4.5.1/4.5.2 - KB3037581 (x64)
1504127	MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure - Windows 8 Gold - .NET Framework 4.5/4.5.1/4.5.2 - KB3037580 (V2.0)
1504129	MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure - Windows 8.1 Gold - .NET Framework 3.5 - KB3037576
1504133	MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB3037573
1504135	MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 3.5 - KB3037576 (x64)
1504201	MS15-042: Vulnerability in Windows Hyper-V Could Allow Denial of Service - Windows 8.1 Gold - KB3047234 (x64)
1504449	MS15-044: Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution - Windows Server 2003 SP2 - .NET Framework 4 - KB3048074 (x64)
1504469	MS15-044: Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution - Windows Server 2003 SP2 - .NET Framework 4 - KB3048074
1504803	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 2008 R2 SP1 / Windows 7 SP1 / Windows 2008 SP2 / Windows Vista SP2 / Windows 2003 SP2 - .NET Framework 4 - KB3023221 (x64)
1504809	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 8.1 Gold - .NET Framework 3.5 - KB3023219
1504813	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 8 Gold - .NET Framework 3.5 - KB3023217
1504817	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2008 R2 SP1 / Windows 7 SP1 - .NET Framework 3.5.1 - KB3023215 (x64)
1504819	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5/4.5.1/4.5.2 - KB3023224
1504825	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 2008 R2 SP1 / Windows 7 SP1 / Windows 2008 SP2 / Windows Vista SP2 / Windows 2003 SP2 - .NET Framework 4 - KB3032662 (x64)
1504829	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 4.5.1 - KB3023222 (x64)

1504831	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 / Windows Server 2003 SP2 - .NET Framework 4 - KB3032662
1504833	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 8 Gold - .NET Framework 3.5 - KB3035486
1504835	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 4.5/4.5.1/4.5.2 - KB3023223 (x64)
1504837	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 7 SP1 - .NET Framework 3.5.1 - KB3023215
1504841	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 8.1 Gold - .NET Framework 4.5.1 - KB3023222
1504843	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB3023213
1504847	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 / Windows Server 2003 SP2 - .NET Framework 4 - KB3023221
1504849	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 3.5 - KB3023217 (x64)
1504853	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB3023213 (x64)
1504855	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 8 Gold - .NET Framework 4.5/4.5.1/4.5.2 - KB3035489 (x64)
1504857	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 3.5 - KB3023219 (x64)
1504863	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5/4.5.1/4.5.2 - KB3023224 (x64)
1504865	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 8 Gold - .NET Framework 4.5/4.5.1/4.5.2 - KB3035489
1504867	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 8 Gold - .NET Framework 3.5 - KB3035486 (x64)
1504871	MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 8 Gold - .NET Framework 4.5/4.5.1/4.5.2 - KB3023223
1505001	MS15-050: Vulnerability in Service Control Manager Could Allow Elevation of Privilege - Windows 7 SP1 - KB3055642 (x64)

1505009	MS15-050: Vulnerability in Service Control Manager Could Allow Elevation of Privilege - Windows 8 Gold - KB3055642
1505011	MS15-050: Vulnerability in Service Control Manager Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3055642
1505013	MS15-050: Vulnerability in Service Control Manager Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3055642 (x64)
1505017	MS15-050: Vulnerability in Service Control Manager Could Allow Elevation of Privilege - Windows Vista SP2 - KB3055642
1505019	MS15-050: Vulnerability in Service Control Manager Could Allow Elevation of Privilege - Windows Vista SP2 - KB3055642 (x64)
1505021	MS15-050: Vulnerability in Service Control Manager Could Allow Elevation of Privilege - Windows 8 Gold - KB3055642 (x64)
1505025	MS15-050: Vulnerability in Service Control Manager Could Allow Elevation of Privilege - Windows 7 SP1 - KB3055642
1505503	MS15-055: Vulnerability in Schannel Could Allow Information Disclosure - Windows 7 SP1 - KB3061518
1505703	MS15-057: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Windows Vista SP2 - Windows Media Player 11 - KB3033890 (x64)
1505709	MS15-057: Vulnerability in Windows Media Player Could Allow Remote Code Execution - Windows Vista SP2 - Windows Media Player 11 - KB3033890
1506001	MS15-060: Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution - Windows 8.1 Gold - KB3059317 (x64)
1506003	MS15-060: Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution - Windows 8 Gold - KB3059317 (x64)
1506007	MS15-060: Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution - Windows 7 SP1 - KB3059317
1506009	MS15-060: Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution - Windows Vista SP2 - KB3059317 (x64)
1506011	MS15-060: Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution - Windows Vista SP2 - KB3059317
1506013	MS15-060: Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution - Windows 8.1 Gold - KB3059317
1506017	MS15-060: Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution - Windows 8 Gold - KB3059317
1506025	MS15-060: Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution - Windows 7 SP1 - KB3059317 (x64)
1506315	MS15-063: Vulnerability in Windows Kernel Could Allow Elevation of Privilege - Windows 8 Gold - KB3063858
1506317	MS15-063: Vulnerability in Windows Kernel Could Allow Elevation of Privilege - Windows 8 Gold - KB3063858 (x64)

1506513	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 6 - KB3065822 (x64)
1506514	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 6 - KB3065822 (x64) - CORRUPT PATCH
1506519	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 7 - KB3065822 (x64)
1506520	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 7 - KB3065822 (x64) - CORRUPT PATCH
1506529	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 6 - KB3065822
1506530	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 6 - KB3065822 - CORRUPT PATCH
1506545	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 8 - KB3065822
1506546	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 8 - KB3065822 - CORRUPT PATCH
1506547	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 7 - KB3065822
1506548	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 7 - KB3065822 - CORRUPT PATCH
1506561	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 8 - KB3065822 (x64)
1506562	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 8 - KB3065822 (x64) - CORRUPT PATCH
1506583	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 8 - KB3074886
1506584	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 8 - KB3074886 - CORRUPT PATCH
1506585	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 7 - KB3074886
1506586	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 7 - KB3074886 - CORRUPT PATCH
1506705	MS15-067: Vulnerability in RDP Could Allow Remote Code Execution - Windows 8 Gold - KB3067904
1506711	MS15-067: Vulnerability in RDP Could Allow Remote Code Execution - Windows 8 Gold - KB3067904 (x64)
1506807	MS15-068: Vulnerabilities in Windows Hyper-V Could Allow Remote Code Execution - Windows 8.1 Gold - KB3046339 (x64)
1506811	MS15-068: Vulnerabilities in Windows Hyper-V Could Allow Remote Code Execution - Windows 8 Gold - KB3046339 (x64)
1506907	MS15-069: Vulnerabilities in Windows Could Allow Remote Code Execution - Windows 8.1 Gold - KB3061512 (x64)

1506911	MS15-069: Vulnerabilities in Windows Could Allow Remote Code Execution - Windows 7 SP1 - KB3067903
1506919	MS15-069: Vulnerabilities in Windows Could Allow Remote Code Execution - Windows 8.1 Gold - KB3061512
1506921	MS15-069: Vulnerabilities in Windows Could Allow Remote Code Execution - Windows Vista SP2 - KB3067903 (x64)
1506925	MS15-069: Vulnerabilities in Windows Could Allow Remote Code Execution - Windows Vista SP2 - KB3067903
1506929	MS15-069: Vulnerabilities in Windows Could Allow Remote Code Execution - Windows 7 SP1 - KB3067903 (x64)
1507403	MS15-074: Vulnerability in Windows Installer Service Could Allow Elevation of Privilege - Windows 8 Gold - KB3072630
1507409	MS15-074: Vulnerability in Windows Installer Service Could Allow Elevation of Privilege - Windows Vista SP2 - KB3072630
1507413	MS15-074: Vulnerability in Windows Installer Service Could Allow Elevation of Privilege - Windows 8 Gold - KB3072630 (x64)
1507415	MS15-074: Vulnerability in Windows Installer Service Could Allow Elevation of Privilege - Windows Vista SP2 - KB3072630 (x64)
1507519	MS15-075: Vulnerabilities in OLE Could Allow Elevation of Privilege - Windows 8 Gold - KB3072633
1507523	MS15-075: Vulnerabilities in OLE Could Allow Elevation of Privilege - Windows 8 Gold - KB3072633 (x64)
1507605	MS15-076: Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege - Windows 8 Gold - KB3067505 (x64)
1507607	MS15-076: Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege - Windows Vista SP2 - KB3067505
1507611	MS15-076: Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege - Windows Vista SP2 - KB3067505 (x64)
1507625	MS15-076: Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege - Windows 8 Gold - KB3067505
1508005	MS15-080: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows 8 Gold - KB3078601
1508027	MS15-080: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 3.0 SP2 - KB3072303
1508029	MS15-080: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows 8 Gold - .NET Framework 3.5 - KB3072306
1508033	MS15-080: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 3.5 - KB3072306 (x64)

1508043	MS15-080: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows 8.1 Gold - .NET Framework 3.5 - KB3072307
1508047	MS15-080: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows 8 Gold - KB3078601 (x64)
1508057	MS15-080: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows Vista SP2 - KB3078601 (x64)
1508061	MS15-080: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 3.5 - KB3072307 (x64)
1508067	MS15-080: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows Vista SP2 - KB3078601
1508087	MS15-080: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows 7 SP1 - .NET Framework 3.5.1 - KB3072305
1508089	MS15-080: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows 7 SP1 - .NET Framework 3.5.1 - KB3072305 (x64)
1508215	MS15-082: Vulnerabilities in RDP Could Allow Remote Code Execution - Windows 8 Gold - KB3075220
1508217	MS15-082: Vulnerabilities in RDP Could Allow Remote Code Execution - Windows Vista SP2 - KB3075221
1508225	MS15-082: Vulnerabilities in RDP Could Allow Remote Code Execution - Windows 7 SP1 - KB3075226 (x64)
1508227	MS15-082: Vulnerabilities in RDP Could Allow Remote Code Execution - Windows Vista SP2 - KB3075221 (x64)
1508231	MS15-082: Vulnerabilities in RDP Could Allow Remote Code Execution - Windows Vista SP2 - KB3075220
1508233	MS15-082: Vulnerabilities in RDP Could Allow Remote Code Execution - Windows 7 SP1 - KB3075226
1508237	MS15-082: Vulnerabilities in RDP Could Allow Remote Code Execution - Windows Vista SP2 - KB3075220 (x64)
1508241	MS15-082: Vulnerabilities in RDP Could Allow Remote Code Execution - Windows 8 Gold - KB3075220 (x64)
1508407	MS15-084: Vulnerabilities in XML Core Services Could Allow Information Disclosure - Windows 8 Gold - KB3076895 (x64)
1508409	MS15-084: Vulnerabilities in XML Core Services Could Allow Information Disclosure - Windows 8.1 Gold - KB3076895
1508413	MS15-084: Vulnerabilities in XML Core Services Could Allow Information Disclosure - Windows Vista SP2 - KB3076895 (x64)
1508417	MS15-084: Vulnerabilities in XML Core Services Could Allow Information Disclosure - Windows 8.1 Gold - KB3076895 (x64)

1508421	MS15-084: Vulnerabilities in XML Core Services Could Allow Information Disclosure - Windows 8 Gold - KB3076895
1508425	MS15-084: Vulnerabilities in XML Core Services Could Allow Information Disclosure - Windows Vista SP2 - KB3076895
1508501	MS15-085: Vulnerability in Mount Manager Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3071756 (x64)
1508503	MS15-085: Vulnerability in Mount Manager Could Allow Elevation of Privilege - Windows 7 SP1 - KB3071756 (x64)
1508505	MS15-085: Vulnerability in Mount Manager Could Allow Elevation of Privilege - Windows 7 SP1 - KB3071756
1508509	MS15-085: Vulnerability in Mount Manager Could Allow Elevation of Privilege - Windows 8 Gold - KB3071756 (x64)
1508515	MS15-085: Vulnerability in Mount Manager Could Allow Elevation of Privilege - Windows Vista SP2 - KB3071756
1508517	MS15-085: Vulnerability in Mount Manager Could Allow Elevation of Privilege - Windows 8 Gold - KB3071756
1508523	MS15-085: Vulnerability in Mount Manager Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3071756
1508525	MS15-085: Vulnerability in Mount Manager Could Allow Elevation of Privilege - Windows Vista SP2 - KB3071756 (x64)
1508807	MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure - Windows 8 Gold - KB3046017 (x64)
1508809	MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure - Windows 7 SP1 - KB3046017
1508819	MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure - Windows 8.1 Gold - KB3046017 (x64)
1508823	MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure - Windows 8 Gold - KB3046017
1508825	MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure - Windows Vista SP2 - KB3046017 (x64)
1508827	MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure - Windows Vista SP2 - KB3046017
1508829	MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure - Windows 7 SP1 - KB3046017 (x64)
1508833	MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure - Windows 8.1 Gold - KB3046017
1508901	MS15-089: Vulnerability in WebDAV Could Allow Information Disclosure - Windows Vista SP2 - KB3076949 (x64)
1508903	MS15-089: Vulnerability in WebDAV Could Allow Information Disclosure - Windows 8 Gold - KB3076949
1508907	MS15-089: Vulnerability in WebDAV Could Allow Information Disclosure - Windows 8.1 Gold - KB3076949

1508909	MS15-089: Vulnerability in WebDAV Could Allow Information Disclosure - Windows Vista SP2 - KB3076949
1508911	MS15-089: Vulnerability in WebDAV Could Allow Information Disclosure - Windows 8 Gold - KB3076949 (x64)
1508913	MS15-089: Vulnerability in WebDAV Could Allow Information Disclosure - Windows 8.1 Gold - KB3076949 (x64)
1509005	MS15-090: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege - Windows 7 SP1 - KB3060716 (x64)
1509007	MS15-090: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege - Windows 8 Gold - KB3060716 (x64)
1509009	MS15-090: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege - Windows 7 SP1 - KB3060716
1509015	MS15-090: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege - Windows Vista SP2 - KB3060716
1509017	MS15-090: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege - Windows 8 Gold - KB3060716
1509021	MS15-090: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege - Windows Vista SP2 - KB3060716 (x64)
1509201	MS15-092: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 8 Gold - .NET Framework 4.6 - KB3083184
1509211	MS15-092: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 4.6 - KB3083184 (x64)
1509707	MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows Vista SP2 - KB3087039
1509711	MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows 8 Gold - KB3087039
1509741	MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows 8 Gold - KB3087039 (x64)
1509751	MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows Vista SP2 - KB3087039 (x64)
1509807	MS15-098: Vulnerabilities in Windows Journal Could Allow Remote Code Execution - Windows 8 Gold - KB3069114 (x64)
1509825	MS15-098: Vulnerabilities in Windows Journal Could Allow Remote Code Execution - Windows 8 Gold - KB3069114
1510101	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5/4.5.1/4.5.2 - KB3074550 (x64)
1510103	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 4.6 - KB3074231 (x64)

1510105	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 8.1 Gold - .NET Framework 4.5.1 - KB3074548
1510107	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4 - KB3074547
1510109	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.6 - KB3074554
1510111	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB3074541 (x64)
1510113	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 7 SP1 - .NET Framework 3.5.1 - KB3074543
1510115	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5/4.5.1/4.5.2 - KB3074230
1510117	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 4.5.1/4.5.2 - KB3074228 (x64)
1510119	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2008 R2 SP1 / Windows 7 SP1 - .NET Framework 3.5.1 - KB3074543 (x64)
1510121	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 8.1 Gold - .NET Framework 4.5.1 - KB3074228
1510123	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 4.5/4.5.1/4.5.2 - KB3074229 (x64)
1510125	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4 - KB3074547 (x64)
1510129	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5/4.5.1/4.5.2 - KB3074230 (x64)
1510131	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 8 Gold - .NET Framework 4.5/4.5.1/4.5.2 - KB3074229
1510133	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.6 - KB3074554 (x64)
1510135	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 8 Gold - .NET Framework 4.6 - KB3074231

1510141	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 8 Gold - .NET Framework 4.6 - KB3074552
1510143	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 3.5 - KB3074545 (x64)
1510145	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 4.5.1 - KB3074548 (x64)
1510147	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.6 - KB3074233
1510149	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5/4.5.1/4.5.2 - KB3074550
1510151	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB3074541
1510153	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 8.1 Gold - .NET Framework 3.5 - KB3074545
1510159	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 8 Gold - .NET Framework 3.5 - KB3074544
1510161	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.6 - KB3074233 (x64)
1510163	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 3.5 - KB3074544 (x64)
1510165	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 4.6 - KB3074552 (x64)
1510167	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 4.5/4.5.1/4.5.2 - KB3074549 (x64)
1510169	MS15-101: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - Windows 8 Gold - .NET Framework 4.5/4.5.1/4.5.2 - KB3074549
1510201	MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege - Windows 8 Gold - KB3082089
1510207	MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege - Windows Vista SP2 - KB3084135
1510211	MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege - Windows Vista SP2 - KB3084135 (x64)

1510213	MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege - Windows 8 Gold - KB3082089 (x64)
1510215	MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege - Windows 8 Gold - KB3084135 (x64)
1510219	MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3082089 (x64)
1510223	MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege - Windows 8 Gold - KB3084135
1510233	MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege - Windows 8.1 Gold - KB3082089
1510903	MS15-109: Security Update for Windows Shell to Address Remote Code Execution - Windows 8 Gold - KB3080446 (x64)
1510905	MS15-109: Security Update for Windows Shell to Address Remote Code Execution - Windows 8 Gold - KB3080446
1510907	MS15-109: Security Update for Windows Shell to Address Remote Code Execution - Windows 7 SP1 - KB3093513 (x64)
1510909	MS15-109: Security Update for Windows Shell to Address Remote Code Execution - Windows 7 SP1 - KB3093513
1510911	MS15-109: Security Update for Windows Shell to Address Remote Code Execution - Windows Vista SP2 - KB3093513
1510925	MS15-109: Security Update for Windows Shell to Address Remote Code Execution - Windows Vista SP2 - KB3093513 (x64)
1511105	MS15-111: Security Update for Windows Kernel to Address Elevation of Privilege - Windows 8 Gold - KB3088195 (x64)
1511109	MS15-111: Security Update for Windows Kernel to Address Elevation of Privilege - Windows 8 Gold - KB3088195
1511115	MS15-111: Security Update for Windows Kernel to Address Elevation of Privilege - Windows 8.1 Gold - KB3088195 (x64)
1511121	MS15-111: Security Update for Windows Kernel to Address Elevation of Privilege - Windows 8.1 Gold - KB3088195
1511701	MS15-117: Security Update for NDIS to Address Elevation of Privilege - Windows Vista SP2 - KB3101722
1511707	MS15-117: Security Update for NDIS to Address Elevation of Privilege - Windows 7 SP1 - KB3101722 (x64)
1511711	MS15-117: Security Update for NDIS to Address Elevation of Privilege - Windows Vista SP2 - KB3101722 (x64)
1511713	MS15-117: Security Update for NDIS to Address Elevation of Privilege - Windows 7 SP1 - KB3101722
1511801	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows 8.1 Gold - .NET Framework 4.6 - KB3098000
1511803	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5/4.5.1/4.5.2 - KB3098781

1511805	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 4.6 - KB3098000 (x64)
1511807	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows 8.1 Gold - .NET Framework 3.5 - KB3097992
1511809	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.6 - KB3098001 (x64)
1511811	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 4.6 - KB3097999 (x64)
1511813	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows 7 SP1 - .NET Framework 3.5.1 - KB3097989
1511815	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows 8.1 Gold - .NET Framework 4.5.1 - KB3098779
1511817	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows 8 Gold - .NET Framework 4.5/4.5.1/4.5.2 - KB3097995
1511819	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows 8 Gold - .NET Framework 3.5 - KB3097991
1511821	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5/4.5.1/4.5.2 - KB3097996
1511823	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows Server 2008 R2 SP1 / Windows 7 SP1 - .NET Framework 3.5.1 - KB3097989 (x64)
1511825	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4 - KB3098778 (x64)
1511827	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 4.5.1 - KB3097997 (x64)
1511829	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 3.5 - KB3097992 (x64)
1511831	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 4.5/4.5.1/4.5.2 - KB3097995 (x64)
1511833	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4 - KB3098778

1511835	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4 - KB3097994 (x64)
1511839	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows 8 Gold - .NET Framework 4.6 - KB3098784
1511841	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 4.5.1 - KB3098779 (x64)
1511843	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.6 - KB3098786 (x64)
1511845	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB3097988
1511847	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 3.5 - KB3097991 (x64)
1511851	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5/4.5.1/4.5.2 - KB3098781 (x64)
1511853	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows Server 2012 Gold / Windows 8 Gold - .NET Framework 4.6 - KB3098784 (x64)
1511855	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.6 - KB3098001
1511857	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows 8 Gold - .NET Framework 4.6 - KB3097999
1511859	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.6 - KB3098786
1511861	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows 8.1 Gold - .NET Framework 4.5.1 - KB3097997
1511863	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB3097988 (x64)
1511869	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4 - KB3097994

1511871	MS15-118: Security Update for .NET Framework to Address Elevation of Privilege - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5/4.5.1/4.5.2 - KB3097996 (x64)
1511901	MS15-119: Security Update for Winsock to Address Elevation of Privilege - Windows 8.1 Gold - KB3092601
1511903	MS15-119: Security Update for Winsock to Address Elevation of Privilege - Windows Vista SP2 - KB3092601
1511907	MS15-119: Security Update for Winsock to Address Elevation of Privilege - Windows 8.1 Gold - KB3092601 (x64)
1511909	MS15-119: Security Update for Winsock to Address Elevation of Privilege - Windows 8 Gold - KB3092601
1511913	MS15-119: Security Update for Winsock to Address Elevation of Privilege - Windows Vista SP2 - KB3092601 (x64)
1511921	MS15-119: Security Update for Winsock to Address Elevation of Privilege - Windows 8 Gold - KB3092601 (x64)
1511923	MS15-119: Security Update for Winsock to Address Elevation of Privilege - Windows 7 SP1 - KB3092601
1511925	MS15-119: Security Update for Winsock to Address Elevation of Privilege - Windows 7 SP1 - KB3092601 (x64)
1512003	MS15-120: Security Update for IPSec to Address Denial of Service - Windows 8 Gold - KB3102939 (x64)
1512005	MS15-120: Security Update for IPSec to Address Denial of Service - Windows 8 Gold - KB3102939
1512009	MS15-120: Security Update for IPSec to Address Denial of Service - Windows 8.1 Gold - KB3102939 (x64)
1512011	MS15-120: Security Update for IPSec to Address Denial of Service - Windows 8.1 Gold - KB3102939
1512109	MS15-121: Security Update for Schannel to Address Spoofing - Windows 8 Gold - KB3081320 (x64)
1512113	MS15-121: Security Update for Schannel to Address Spoofing - Windows 8 Gold - KB3081320
1512115	MS15-121: Security Update for Schannel to Address Spoofing - Windows 8.1 Gold - KB3081320 (x64)
1512123	MS15-121: Security Update for Schannel to Address Spoofing - Windows 8.1 Gold - KB3081320
1512461	3125869: Vulnerability in Internet Explorer could lead to ASLR bypass - Enable the User32 Exception Handler Hardening Feature
1512801	MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution - Windows Vista SP2 - KB3109094 (x64)

1512803	MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution - Windows 8 Gold - .NET Framework 3.5 - KB3099863 (x64)
1512811	MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5/4.5.1 - KB3099869
1512823	MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5/4.5.1 - KB3099869 (x64)
1512825	MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution - Windows Vista SP2 - KB3109094
1512829	MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution - Windows 8 Gold - .NET Framework 3.5 - KB3099863
1512833	MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4 - KB3099866 (x64)
1512851	MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4 - KB3099866
1512859	MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution - Windows 8 Gold - KB3109094 (x64)
1512871	MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution - Windows 8 Gold - KB3109094
1513205	MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 7 SP1 - KB3108371 (x64)
1513207	MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8 Gold - KB3108347
1513209	MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution - Windows Vista SP2 - KB3108371
1513215	MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8 Gold - KB3108381
1513223	MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 7 SP1 - KB3108371
1513225	MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution - Windows Vista SP2 - KB3108371 (x64)
1513227	MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution - Windows Vista SP2 - KB3108381 (x64)
1513233	MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution - Windows Vista SP2 - KB3108381
1513235	MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8 Gold - KB3108381 (x64)

1513237	MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8 Gold - KB3108347 (x64)
1513243	MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 7 SP1 - KB3108381 (x64)
1513249	MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 7 SP1 - KB3108381
1513301	MS15-133: Security Update for Windows PGM to Address Elevation of Privilege - Windows 7 SP1 - KB3109103 (x64)
1513305	MS15-133: Security Update for Windows PGM to Address Elevation of Privilege - Windows 8.1 Gold - KB3109103 (x64)
1513309	MS15-133: Security Update for Windows PGM to Address Elevation of Privilege - Windows 8 Gold - KB3109103 (x64)
1513311	MS15-133: Security Update for Windows PGM to Address Elevation of Privilege - Windows 8 Gold - KB3109103
1513315	MS15-133: Security Update for Windows PGM to Address Elevation of Privilege - Windows Vista SP2 - KB3109103 (x64)
1513317	MS15-133: Security Update for Windows PGM to Address Elevation of Privilege - Windows 8.1 Gold - KB3109103
1513319	MS15-133: Security Update for Windows PGM to Address Elevation of Privilege - Windows 7 SP1 - KB3109103
1513323	MS15-133: Security Update for Windows PGM to Address Elevation of Privilege - Windows Vista SP2 - KB3109103
1513405	MS15-134: Security Update for Windows Media Center to Address Remote Code Execution - Windows 8 Gold - Windows Media Center - KB3108669
1513407	MS15-134: Security Update for Windows Media Center to Address Remote Code Execution - Windows 8 Gold - Windows Media Center - KB3108669 (x64)
1513503	MS15-135: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege - Windows Vista SP2 - KB3109094 (x64)
1513505	MS15-135: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege - Windows Vista SP2 - KB3109094
1513507	MS15-135: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege - Windows 8 Gold - KB3109094
1513519	MS15-135: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege - Windows 8 Gold - KB3109094 (x64)
1576801	UPDATE: Microsoft .NET Framework 3.0 Available - Windows XP/2003/Vista
1576802	UPDATE: Microsoft .NET Framework 3.0 SP1 Available - Windows XP/2003/Vista
1576805	UPDATE: Microsoft .NET Framework 3.0 Service Pack 1 Redistributable Available - Windows XP/2003

1576809	UPDATE: Microsoft .NET Framework 3.0 SP1 Available - Windows XP/2003/Vista (x64)
1600103	MS16-001: Cumulative Security Update for Internet Explorer - Windows Server 2008 R2 SP1 - IE 10 - KB3124275 (x64)
1600117	MS16-001: Cumulative Security Update for Internet Explorer - Windows Server 2008 R2 SP1 - IE 9 - KB3124275 (x64)
1600121	MS16-001: Cumulative Security Update for Internet Explorer - Windows Server 2008 SP2 - IE 7 - KB3124275 (x64)
1600123	MS16-001: Cumulative Security Update for Internet Explorer - Windows Server 2008 SP2 - IE 8 - KB3124275 (x64)
1600125	MS16-001: Cumulative Security Update for Internet Explorer - Windows Server 2008 SP2 - IE 8 - KB3124275
1600127	MS16-001: Cumulative Security Update for Internet Explorer - Windows Vista SP2 - IE 7 - KB3124275 (x64)
1600133	MS16-001: Cumulative Security Update for Internet Explorer - Windows Server 2008 SP2 - IE 7 - KB3124275
1600137	MS16-001: Cumulative Security Update for Internet Explorer - Windows Vista SP2 - IE 7 - KB3124275
1600139	MS16-001: Cumulative Security Update for Internet Explorer - Windows Server 2008 R2 SP1 - IE 8 - KB3124275 (x64)
1600143	MS16-001: Cumulative Security Update for Internet Explorer - Windows Vista SP2 - IE 8 - KB3124275
1600147	MS16-001: Cumulative Security Update for Internet Explorer - Windows Vista SP2 - IE 8 - KB3124275 (x64)
1600507	MS16-005: Security Update for Windows Kernel-Mode Drivers to Address Remote Code Execution - Windows 8 Gold - KB3124001
1600529	MS16-005: Security Update for Windows Kernel-Mode Drivers to Address Remote Code Execution - Windows 8 Gold - KB3124001 (x64)
1600703	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 7 SP1 - KB3121461 (x64)
1600705	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8.1 Gold - KB3121461
1600707	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows Vista SP2 - KB3108664 (x64)
1600711	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8 Gold - KB3121918
1600713	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 7 SP1 - KB3110329 (x64)
1600719	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows Vista SP2 - KB3110329 (x64)
1600723	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 7 SP1 - KB3109560

1600729	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8 Gold - KB3121918 (x64)
1600737	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 7 SP1 - KB3108664
1600739	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8.1 Gold - KB3110329 (x64)
1600741	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8.1 Gold - KB3109560 (x64)
1600745	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8 Gold - KB3110329
1600747	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8.1 Gold - KB3109560
1600749	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8 Gold - KB3109560 (x64)
1600751	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows Vista SP2 - KB3108664
1600755	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8.1 Gold - KB3121461 (x64)
1600765	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8 Gold - KB3121461 (x64)
1600767	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 7 SP1 - KB3108664 (x64)
1600773	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8.1 Gold - KB3110329
1600775	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8 Gold - KB3110329 (x64)
1600777	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows Vista SP2 - KB3109560 (x64)
1600779	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 7 SP1 - KB3109560 (x64)
1600785	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows Vista SP2 - KB3110329
1600787	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 7 SP1 - KB3121461
1600789	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 7 SP1 - KB3110329
1600795	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows Vista SP2 - KB3109560
1600797	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8 Gold - KB3121461
1600799	MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8 Gold - KB3109560

1600805	MS16-008: Security Update for Windows Kernel to Address Elevation of Privilege - Windows 8 Gold - KB3121212
1600819	MS16-008: Security Update for Windows Kernel to Address Elevation of Privilege - Windows 8 Gold - KB3121212 (x64)
1601301	MS16-013: Security Update for Windows Journal to Address Remote Code Execution - Windows 8.1 Gold - KB3115858
1601305	MS16-013: Security Update for Windows Journal to Address Remote Code Execution - Windows 7 SP1 - KB3115858
1601309	MS16-013: Security Update for Windows Journal to Address Remote Code Execution - Windows Vista SP2 - KB3115858
1601313	MS16-013: Security Update for Windows Journal to Address Remote Code Execution - Windows 7 SP1 - KB3115858 (x64)
1601315	MS16-013: Security Update for Windows Journal to Address Remote Code Execution - Windows Vista SP2 - KB3115858 (x64)
1601319	MS16-013: Security Update for Windows Journal to Address Remote Code Execution - Windows 8.1 Gold - KB3115858 (x64)
1601403	MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8.1 Gold - KB3126587
1601407	MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8.1 Gold - KB3126434 (x64)
1601409	MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8.1 Gold - KB3126593 (x64)
1601411	MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution - Windows Vista SP2 - KB3126587
1601427	MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8.1 Gold - KB3126587 (x64)
1601431	MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 7 SP1 - KB3126587
1601433	MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 7 SP1 - KB3126593 (x64)
1601435	MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8.1 Gold - KB3126593
1601437	MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 7 SP1 - KB3126593
1601441	MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 8.1 Gold - KB3126434
1601447	MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution - Windows Vista SP2 - KB3126587 (x64)
1601449	MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution - Windows 7 SP1 - KB3126587 (x64)

1601905	MS16-019: Security Update for .NET Framework to Address Denial of Service - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5.2 - KB3127229 (x64)
1601911	MS16-019: Security Update for .NET Framework to Address Denial of Service - Windows 7 SP1 - .NET Framework 3.5.1 - KB3127220
1601921	MS16-019: Security Update for .NET Framework to Address Denial of Service - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 3.5 - KB3127222 (x64)
1601923	MS16-019: Security Update for .NET Framework to Address Denial of Service - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.6/4.6.1 - KB3127233
1601929	MS16-019: Security Update for .NET Framework to Address Denial of Service - Windows Vista SP2 - .NET Framework 2.0 SP2 - KB3127219
1601937	MS16-019: Security Update for .NET Framework to Address Denial of Service - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5.2 - KB3127229
1601945	MS16-019: Security Update for .NET Framework to Address Denial of Service - Windows Server 2008 R2 SP1 / Windows 7 SP1 - .NET Framework 3.5.1 - KB3127220 (x64)
1601947	MS16-019: Security Update for .NET Framework to Address Denial of Service - Windows 8.1 Gold - .NET Framework 3.5 - KB3127222
1601961	MS16-019: Security Update for .NET Framework to Address Denial of Service - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.6/4.6.1 - KB3127233 (x64)
1602503	MS16-025: Security Update for Windows Library Loading to Address Remote Code Execution - Windows Vista SP2 - KB3140709
1602505	MS16-025: Security Update for Windows Library Loading to Address Remote Code Execution - Windows Vista SP2 - KB3140709 (x64)
1602711	MS16-027: Security Update for Windows Media to Address Remote Code Execution - Windows 7 SP1 - KB3138910
1602713	MS16-027: Security Update for Windows Media to Address Remote Code Execution - Windows 8.1 Gold - KB3138910
1602717	MS16-027: Security Update for Windows Media to Address Remote Code Execution - Windows 8.1 Gold - KB3138962
1602721	MS16-027: Security Update for Windows Media to Address Remote Code Execution - Windows 7 SP1 - KB3138910 (x64)
1602723	MS16-027: Security Update for Windows Media to Address Remote Code Execution - Windows 8.1 Gold - KB3138962 (x64)
1602725	MS16-027: Security Update for Windows Media to Address Remote Code Execution - Windows 8.1 Gold - KB3138910 (x64)

1603201	MS16-032: Security Update for Secondary Logon to Address Elevation of Privilege - Windows 8.1 Gold - KB3139914 (x64)
1603205	MS16-032: Security Update for Secondary Logon to Address Elevation of Privilege - Windows Vista SP2 - KB3139914
1603207	MS16-032: Security Update for Secondary Logon to Address Elevation of Privilege - Windows Vista SP2 - KB3139914 (x64)
1603211	MS16-032: Security Update for Secondary Logon to Address Elevation of Privilege - Windows 7 SP1 - KB3139914 (x64)
1603213	MS16-032: Security Update for Secondary Logon to Address Elevation of Privilege - Windows 8.1 Gold - KB3139914
1603221	MS16-032: Security Update for Secondary Logon to Address Elevation of Privilege - Windows 7 SP1 - KB3139914
1603301	MS16-033: Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege - Windows 8.1 Gold - KB3139398 (x64)
1603303	MS16-033: Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege - Windows 8.1 Gold - KB3139398
1603313	MS16-033: Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege - Windows 7 SP1 - KB3139398 (x64)
1603315	MS16-033: Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege - Windows Vista SP2 - KB3139398
1603317	MS16-033: Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege - Windows Vista SP2 - KB3139398 (x64)
1603319	MS16-033: Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege - Windows 7 SP1 - KB3139398
1603323	MS16-033: Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege - Windows Embedded Standard 7 - KB3139398
1603325	MS16-033: Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege - Windows Embedded Standard 7 - KB3139398 (x64)
1603501	MS16-035: Security Update for .NET Framework to Address Security Feature Bypass - Windows Server 2008 R2 SP1 / Windows 7 SP1 - .NET Framework 3.5.1 - KB3135983 (x64)
1603503	MS16-035: Security Update for .NET Framework to Address Security Feature Bypass - Windows 8.1 Gold - .NET Framework 4.5.2 - KB3135994
1603511	MS16-035: Security Update for .NET Framework to Address Security Feature Bypass - Windows 8.1 Gold - .NET Framework 3.5 - KB3135985
1603519	MS16-035: Security Update for .NET Framework to Address Security Feature Bypass - Windows 7 SP1 - .NET Framework 3.5.1 - KB3135983
1603523	MS16-035: Security Update for .NET Framework to Address Security Feature Bypass - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 4.5.2 - KB3135994 (x64)

1603525	MS16-035: Security Update for .NET Framework to Address Security Feature Bypass - Windows Server 2012 R2 Gold / Windows 8.1 Gold - .NET Framework 3.5 - KB3135985 (x64)
1603533	MS16-035: Security Update for .NET Framework to Address Security Feature Bypass - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5.2 - KB3135996
1603539	MS16-035: Security Update for .NET Framework to Address Security Feature Bypass - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB3135982
1603541	MS16-035: Security Update for .NET Framework to Address Security Feature Bypass - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5.2 - KB3135996 (x64)
1603543	MS16-035: Security Update for .NET Framework to Address Security Feature Bypass - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB3135982 (x64)
1603553	MS16-035: Security Update for .NET Framework to Address Security Feature Bypass - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.6/4.6.1 - KB3136000 (x64)
1603565	MS16-035: Security Update for .NET Framework to Address Security Feature Bypass - Windows Server 2012 R2 / Windows 8.1 - .NET Framework 4.5.2 - LDR Branch - KB3135994 (x64)
1603575	MS16-035: Security Update for .NET Framework to Address Security Feature Bypass - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.6/4.6.1 - KB3136000
1603583	MS16-035: Security Update for .NET Framework to Address Security Feature Bypass - Windows 8.1 - .NET Framework 4.5.2 - LDR Branch - KB3135994
1604101	MS16-041: Security Update for .NET Framework - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.6/4.6.1 - KB3143693
1604103	MS16-041: Security Update for .NET Framework - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.6/4.6.1 - KB3143693 (x64)
1604701	MS16-047: Security Update for SAM and LSAD Remote Protocols - Windows 7 SP1 - KB3149090 (x64)
1604703	MS16-047: Security Update for SAM and LSAD Remote Protocols - Windows 8.1 Gold - KB3149090
1604707	MS16-047: Security Update for SAM and LSAD Remote Protocols - Windows Vista SP2 - KB3149090
1604709	MS16-047: Security Update for SAM and LSAD Remote Protocols - Windows 8.1 Gold - KB3149090 (x64)

1604715	MS16-047: Security Update for SAM and LSAD Remote Protocols - Windows Vista SP2 - KB3149090 (x64)
1604719	MS16-047: Security Update for SAM and LSAD Remote Protocols - Windows 7 SP1 - KB3149090
1604801	MS16-048: Security Update for CSRSS - Windows 8.1 Gold - KB3146723
1604805	MS16-048: Security Update for CSRSS - Windows 8.1 Gold - KB3146723 (x64)
1605501	MS16-055: Security Update for Microsoft Graphics Component - Windows 7 SP1 - KB3156016
1605543	MS16-055: Security Update for Microsoft Graphics Component - Windows 7 SP1 - KB3156016 (x64)
1605545	MS16-055: Security Update for Microsoft Graphics Component - Windows Vista SP2 - KB3156019 (x64)
1605561	MS16-055: Security Update for Microsoft Graphics Component - Windows Vista SP2 - KB3156019
1605601	MS16-056: Security Update for Windows Journal - Windows 8.1 - KB3155178 (x64)
1605603	MS16-056: Security Update for Windows Journal - Windows Vista SP2 - KB3155178 (x64)
1605605	MS16-056: Security Update for Windows Journal - Windows 7 SP1 - KB3155178 (x64)
1605607	MS16-056: Security Update for Windows Journal - Windows Vista SP2 - KB3155178
1605609	MS16-056: Security Update for Windows Journal - Windows 7 SP1 - KB3155178
1605611	MS16-056: Security Update for Windows Journal - Windows 8.1 - KB3155178
1605701	MS16-057: Security Update for Windows Shell - Windows 8.1 - KB3156059 (x64)
1605705	MS16-057: Security Update for Windows Shell - Windows 8.1 - KB3156059
1605803	MS16-058: Security Update for Windows IIS - Windows Vista SP2 - KB3141083 (x64)
1605807	MS16-058: Security Update for Windows IIS - Windows Vista SP2 - KB3141083
1605905	MS16-059: Security Update for Windows Media Center - Windows Vista SP2 - Windows Media Center - KB3150220 (x64)
1605907	MS16-059: Security Update for Windows Media Center - Windows 7 SP1 - Windows Media Center - KB3150220
1605909	MS16-059: Security Update for Windows Media Center - Windows 7 SP1 - Windows Media Center - KB3150220 (x64)
1605911	MS16-059: Security Update for Windows Media Center - Windows Vista SP2 - Windows Media Center - KB3150220

1606207	MS16-062: Security Update for Windows Kernel-Mode Drivers - Windows Vista SP2 - KB3156017 (x64)
1606243	MS16-062: Security Update for Windows Kernel-Mode Drivers - Windows Vista SP2 - KB3156017
1606503	MS16-065: Security Update for .NET Framework - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB3142023(Superseded)
1607203	MS16-072: Security Update for Group Policy - Windows 7 SP1 - KB3159398
1607205	MS16-072: Security Update for Group Policy - Windows Vista SP2 - KB3159398 (x64)
1607209	MS16-072: Security Update for Group Policy - Windows Vista SP2 - KB3159398
1607211	MS16-072: Security Update for Group Policy - Windows 8.1 - KB3159398 (x64)
1607213	MS16-072: Security Update for Group Policy - Windows 8.1 - KB3159398
1607221	MS16-072: Security Update for Group Policy - Windows 7 SP1 - KB3159398 (x64)
1607507	MS16-075: Security Update for Windows SMB Server - Windows Vista SP2 - KB3161561 (x64)
1607521	MS16-075: Security Update for Windows SMB Server - Windows Vista SP2 - KB3161561
1607701	MS16-077: Security Update for WPAD - Windows 7 SP1 - KB3161949
1607707	MS16-077: Security Update for WPAD - Windows Vista SP2 - KB3161949 (x64)
1607709	MS16-077: Security Update for WPAD - Windows 8.1 - KB3161949 (x64)
1607711	MS16-077: Security Update for WPAD - Windows 7 SP1 - KB3161949 (x64)
1607713	MS16-077: Security Update for WPAD - Windows Vista SP2 - KB3161949
1607715	MS16-077: Security Update for WPAD - Windows 8.1 - KB3161949
1608605	MS16-086: Cumulative Security Update for JScript and VBScript - Windows Vista SP2 - VBScript 5.7 - KB3169659
1608607	MS16-086: Cumulative Security Update for JScript and VBScript - Windows Vista SP2 - VBScript 5.7 - KB3169659 (x64)
1608705	MS16-087: Security Update for Windows Print Spooler Components - Windows Vista SP2 - KB3170455
1608717	MS16-087: Security Update for Windows Print Spooler Components - Windows Vista SP2 - KB3170455 (x64)
1609101	MS16-091: Security Update for .NET Framework - Windows Server 2008 R2 SP1 / Windows 7 SP1 - .NET Framework 3.5.1 - KB3163245 (x64)
1609103	MS16-091: Security Update for .NET Framework - Windows Server 2008 R2 SP1 / Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5.2 - KB3163251 (x64)

1609111	MS16-091: Security Update for .NET Framework - Windows 7 SP1 - .NET Framework 3.5.1 - KB3163245
1609125	MS16-091: Security Update for .NET Framework - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5.2 - KB3163251
1610001	MS16-100: Security Update for Secure Boot - Windows 8.1 - KB3172729
1610129	MS16-101: Description of the security update for Windows authentication methods - Windows Server 2008 / Windows Vista - KB3167679 (V2.0)
1610131	MS16-101: Description of the security update for Windows authentication methods - Windows Server 2008 / Windows Vista - KB3167679 (x64) (V2.0)
1610605	MS16-106: Security Update for Microsoft Graphics Component - Windows Vista SP2 - KB3185911 (x64)
1610609	MS16-106: Security Update for Microsoft Graphics Component - Windows Vista SP2 - KB3185911
1611115	MS16-111: Security Update for Windows Kernel - Windows 8.1 - KB3175024 (x64)
1611117	MS16-111: Security Update for Windows Kernel - Windows 8.1 - KB3175024
1611211	MS16-112: Security Update for Windows Lock Screen - Windows 8.1 - KB3178539 (x64)
1611215	MS16-112: Security Update for Windows Lock Screen - Windows 8.1 - KB3178539
1611411	MS16-114: Security Update for Windows SMBv1 Server - Windows Vista SP2 - KB3177186 (x64)
1611413	MS16-114: Security Update for Windows SMBv1 Server - Windows Vista SP2 - KB3177186
1612015	MS16-120: Security Update for Microsoft Graphics Component - Security Only - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 3.0 SP2 - KB3188726 (x64) (Superseded)
1612017	MS16-120: Security Update for Microsoft Graphics Component - Security Only - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 3.0 SP2 - KB3188726 (Superseded)
1612039	MS16-120: Security Update for Microsoft Graphics Component - Security Only - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5.2 - KB3189039 (x64)
1612041	MS16-120: Security Update for Microsoft Graphics Component - Security Only - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.5.2 - KB3189039
1612043	MS16-120: Security Update for Microsoft Graphics Component - Security Only - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.6 - KB3189040 (x64)

1612045	MS16-120: Security Update for Microsoft Graphics Component - Security Only - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 4.6 - KB3189040
1612075	MS16-120: Security Update for Microsoft Graphics Component - Monthly Rollup - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 3.0 SP2 - KB3188735 (x64)
1612077	MS16-120: Security Update for Microsoft Graphics Component - Monthly Rollup - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 3.0 SP2 - KB3188735
1612301	MS16-123: Security Update for Windows Kernel-Mode Drivers - Windows Server 2008 SP2 / Windows Vista SP2 - KB3183431 (x64)
1612303	MS16-123: Security Update for Windows Kernel-Mode Drivers - Windows Server 2008 SP2 / Windows Vista SP2 - KB3183431
1613001	MS16-130: Security Update for Microsoft Windows - Windows Server 2008 SP2 / Windows Vista SP2 - KB3193418 (x64)
1613003	MS16-130: Security Update for Microsoft Windows - Windows Server 2008 SP2 / Windows Vista SP2 - KB3193418
1613005	MS16-130: Security Update for Microsoft Windows - Windows Server 2008 SP2 / Windows Vista SP2 - KB3196718 (x64)
1613007	MS16-130: Security Update for Microsoft Windows - Windows Server 2008 SP2 / Windows Vista SP2 - KB3196718
1613101	MS16-131: Security Update for Microsoft Video Control - Windows Vista SP2 - KB3198218 (x64)
1613103	MS16-131: Security Update for Microsoft Video Control - Windows Vista SP2 - KB3198218
1613501	MS16-135: Security Update for Windows Kernel-Mode Drivers - Windows Server 2008 SP2 / Windows Vista SP2 - KB3194371 (x64)
1613503	MS16-135: Security Update for Windows Kernel-Mode Drivers - Windows Server 2008 SP2 / Windows Vista SP2 - KB3194371
1614301	MS17-JUN: Security update for Windows XP and Windows Server 2003 - Windows Server 2003 SP2 / Windows XP SP2 - KB3197835 (x64)
1614303	MS17-JUN: Security update for Windows XP and Windows Server 2003 - Windows Server 2003 SP2 - KB3197835
1614305	MS17-JUN: Security update for Windows XP and Windows Server 2003 - Windows XP SP3 - KB3197835
1614409	MS16-144: Cumulative Security Update for Internet Explorer - Windows Server 2008 SP2 - Windows Hyperlink Object Library - KB3208481 (x64)
1614411	MS16-144: Cumulative Security Update for Internet Explorer - Windows Vista SP2 - Windows Hyperlink Object Library - KB3208481 (x64)
1614413	MS16-144: Cumulative Security Update for Internet Explorer - Windows Vista SP2 - Windows Hyperlink Object Library - KB3208481
1614415	MS16-144: Cumulative Security Update for Internet Explorer - Windows Server 2008 SP2 - Windows Hyperlink Object Library - KB3208481

1614609	MS16-146: Security Update for Microsoft Graphics Component - Windows Vista SP2 - KB3205638 (x64)
1614615	MS16-146: Security Update for Microsoft Graphics Component - Windows Vista SP2 - KB3205638
1614903	MS16-149: Security Update for Microsoft Windows - Windows Vista SP2 - KB3196726
1614907	MS16-149: Security Update for Microsoft Windows - Windows Vista SP2 - KB3196726 (x64)
1615301	MS16-153: Security Update for Common Log File System Driver - Windows Vista SP2 - KB3203838 (x64)
1615305	MS16-153: Security Update for Common Log File System Driver - Windows Vista SP2 - KB3203838
1615545	MS16-155: Security Update for .NET Framework - Security Only - Windows 7 SP1 / Windows Server 2008 R2 SP1 - .NET Framework 4.6.2 - KB3204805 (x64)
1615547	MS16-155: Security Update for .NET Framework - Security Only - Windows 7 SP1 - .NET Framework 4.6.2 - KB3204805
1615551	MS16-155: Security Update for .NET Framework - Security Only - Windows 8.1 - .NET Framework 4.6.2 - KB3204802 (x64)
1615557	MS16-155: Security Update for .NET Framework - Security Only - Windows 8.1 - .NET Framework 4.6.2 - KB3204802
1700407	MS17-004: Security Update for Local Security Authority Subsystem Service - Windows Vista SP2 - KB3216775 (x64)
1700413	MS17-004: Security Update for Local Security Authority Subsystem Service - Windows Vista SP2 - KB3216775
1700601	MS17-006: Cumulative Security Update for Internet Explorer - Windows Server 2008 SP2 - Microsoft Internet Messaging API - KB3218362 (x64)
1700603	MS17-006: Cumulative Security Update for Internet Explorer - Windows Vista SP2 - Microsoft Internet Messaging API - KB3218362 (x64)
1700605	MS17-006: Cumulative Security Update for Internet Explorer - Windows Vista SP2 - Microsoft Internet Messaging API - KB3218362
1700607	MS17-006: Cumulative Security Update for Internet Explorer - Windows Server 2008 SP2 - Microsoft Internet Messaging API - KB3218362
1700633	MS17-008, MS17-010, MS17-011, MS17-012, MS17-013, MS17-016, MS17-017, MS17-018, MS17-020, MS17-021, MS17-022: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4012212 (x64)
1700635	MS17-008, MS17-010, MS17-011, MS17-012, MS17-013, MS17-016, MS17-017, MS17-018, MS17-020, MS17-021, MS17-022: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4012212
1700639	MS17-008, MS17-009, MS17-010, MS17-011, MS17-012, MS17-013, MS17-016, MS17-017, MS17-018, MS17-021, MS17-022: Security Only Quality Update - Security Only - Windows 8.1 - KB4012213 (x64)

1700641	MS17-008, MS17-009, MS17-010, MS17-011, MS17-012, MS17-013, MS17-016, MS17-017, MS17-018, MS17-021, MS17-022: Security Only Quality Update - Security Only - Windows 8.1 - KB4012213
1701001	MS17-010: Security Update for Microsoft Windows SMB Server - Windows Vista SP2 - KB4012598 (x64)
1701007	MS17-010: Security Update for Microsoft Windows SMB Server - Windows Vista SP2 - KB4012598
1701009	MS17-010: Security Update for Windows SMB Server - Windows 8 - KB4012598
1701011	MS17-010: Security Update for Windows SMB Server - Windows 8 - KB4012598 (x64)
1701017	MS17-010: Security update for Windows SMB Server - Windows XP SP2 - KB4012598 (x64)
1701019	MS17-010: Security update for Windows SMB Server - Windows XP SP3 - KB4012598
1701203	MS17-012: Security Update for Microsoft Windows - Windows Vista SP2 - KB3217587 (x64)
1701205	MS17-012: Security Update for Microsoft Windows - Windows Vista SP2 - KB3217587
1701333	MS17-013: Security Update for Microsoft Graphics Component - Windows Vista SP2 - KB4012584 (x64)
1701339	MS17-013: Security Update for Microsoft Graphics Component - Windows Vista SP2 - KB4012584
1701369	MS17-JUN: Security update for Microsoft Graphics Component - Windows 8 - KB4012583 (x64)
1701371	MS17-JUN: Security update for Microsoft Graphics Component - Windows 8 - KB4012583
1701373	MS17-JUN: Security update for Microsoft Graphics Component - Windows Server 2003 SP2 / Windows XP SP2 - KB4012583 (x64)
1701375	MS17-JUN: Security update for Microsoft Graphics Component - Windows XP SP3 - KB4012583
1701601	MS17-016: Security Update for Windows IIS - Windows Vista SP2 - KB4012373 (x64)
1701605	MS17-016: Security Update for Windows IIS - Windows Vista SP2 - KB4012373
1702001	MS17-020: Security Update for Windows DVD Maker - Windows Vista SP2 - KB3205715 (x64)
1702003	MS17-020: Security Update for Windows DVD Maker - Windows Vista SP2 - KB3205715
1702201	MS17-022: Security Update for Microsoft XML Core Services - Windows Vista SP2 - Microsoft XML Core Services 3.0 - KB3216916 (x64)
1702207	MS17-022: Security Update for Microsoft XML Core Services - Windows Vista SP2 - Microsoft XML Core Services 3.0 - KB3216916

2000401	MS00-004: Patch Available for "RDISK Registry Enumeration File" Vulnerability
2000501	MS00-005: "Malformed RTF Control Word" Vulnerability in Windows 98 and 98 SE
2001601	MS00-016: Malformed Media License Request Vulnerability
2003801	MS00-038: Malformed Windows Media Encoder Request Vulnerability
2005401	MS00-054: "Malformed IPX Ping Packet" Vulnerability in Windows 98 (IPX installed)
2005402	MS00-054: "Malformed IPX Ping Packet" Vulnerability in Windows 98 (IPX installed) - CORRUPT PATCH
2005403	MS00-054: "Malformed IPX Ping Packet" Vulnerability (IPX not installed)
2005404	MS00-054: "Malformed IPX Ping Packet" Vulnerability in Windows 95 (IPX installed)
2005405	MS00-054: "Malformed IPX Ping Packet" Vulnerability in Windows 95 (IPX installed) - CORRUPT PATCH
2007201	MS00-072: "Share Level Password" Vulnerability in Windows 98
2007202	MS00-072: "Share Level Password" Vulnerability in Windows 98 - CORRUPT PATCH
2007203	MS00-072: "Share Level Password" Vulnerability in Windows 98SE
2007204	MS00-072: "Share Level Password" Vulnerability in Windows 98SE - CORRUPT PATCH
2007205	MS00-072: "Share Level Password" Vulnerability in Windows ME
2007206	MS00-072: "Share Level Password" Vulnerability in Windows ME - CORRUPT PATCH
2007301	MS00-073: Malformed IPX NMPI Packet Vulnerability in Windows 98
2007302	MS00-073: Malformed IPX NMPI Packet Vulnerability in Windows 98 - CORRUPT PATCH
2007303	MS00-073: Malformed IPX NMPI Packet Vulnerability in Windows 98SE
2007304	MS00-073: Malformed IPX NMPI Packet Vulnerability in Windows 98SE - CORRUPT PATCH
2007305	MS00-073: Malformed IPX NMPI Packet Vulnerability in Windows ME
2007306	MS00-073: Malformed IPX NMPI Packet Vulnerability in Windows ME - CORRUPT PATCH
2007307	MS00-073: Malformed IPX NMPI Packet Vulnerability in Windows 95
2007308	MS00-073: Malformed IPX NMPI Packet Vulnerability in Windows 95 - CORRUPT PATCH
2007401	MS00-074: "WebTV for Windows Denial of Service" Vulnerability
2007402	MS00-074: "WebTV for Windows Denial of Service" Vulnerability - CORRUPT PATCH
2007403	MS00-074: "WebTV" for Windows Denial of Service" Vulnerability
2007404	MS00-074: "WebTV" for Windows Denial of Service" Vulnerability - CORRUPT PATCH

2007901	MS00-079: "HyperTerminal Buffer Overflow" Vunlerability in Windows ME
2007902	MS00-079: "HyperTerminal Buffer Overflow" Vunlerability in Windows ME - CORRUPT PATCH
2007905	MS00-079: "Hyper Terminal Buffer Overflow" Vulnerability in Windows NT
2007906	MS00-079: "Hyper Terminal Buffer Overflow" Vulnerability in Windows NT - CORRUPT PATCH
2008701	MS00-087: Terminal Server Login Buffer Overflow Vulnerability
2008702	MS00-087: Terminal Server Login Buffer Overflow Vulnerability - CORRUPT PATCH
2009101	MS00-091: Incomplete TCP/IP Packet Vulnerability
2009102	MS00-091: Incomplete TCP/IP Vulnerability in Windows NT 4.0 Terminal Server Edition
2009501	MS00-095: Registry Permissions Vulnerability
2009701	MS00-097: Severed Windows Media Server Connection Vulnerability
6012022	MS06-012: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution - Office 2000 MUI - Windows NT/2000/XP/2003 (Administrative Installation)
9062139	MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution - Visual FoxPro 8.0 SP1 - Windows 2000 SP4
9062140	MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution - Visual FoxPro 8.0 SP1 - Windows 2000 SP4 - CORRUPT PATCH
9062141	MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution - Visual FoxPro 9.0 SP2- Windows 2000 SP4
9062142	MS09-062: Vulnerabilities in GDI+ Could Allow Remote Code Execution - Visual FoxPro 9.0 SP2- Windows 2000 SP4 - CORRUPT PATCH
9901001	MS99-010: File Access Vulnerability in FrontPage 98 Personal Web Server
9901002	MS99-010: File Access Vulnerability in FrontPage 97 Personal Web Server
9903303	MS99-033: "Malformed Telnet Argument" Patch for Windows 95 Telnet Client
9903304	MS99-033: "Malformed Telnet Argument" Patch for Windows 95 Telnet Client - CORRUPT PATCH
9903601	MS99-036: Windows NT 4.0 Does Not Delete Unattended Installation File $winnt$.inf
9903602	MS99-036: Windows NT 4.0 Does Not Delete Unattended Installation File $nt4pre$.inf
9903603	MS99-036: Windows NT 4.0 Does Not Delete Unattended Installation Files
9903801	MS99-038,034: "Spoofed Route Pointer" and "Fragmented IGMP Packet" Vulnerabilities - Windows 98

9903802	MS99-038,034: "Spoofed Route Pointer" and "Fragmented IGMP Packet" Vulnerabilities - Windows 98 SE
9903803	MS99-038,034: "Spoofed Route Pointer" and "Fragmented IGMP Packet" Vulnerabilities - Windows 98 - CORRUPT PATCH
9903804	MS99-038,034: "Spoofed Route Pointer" and "Fragmented IGMP Packet" Vulnerabilities - Windows 98 SE - CORRUPT PATCH
9903805	MS99-038,034: "Spoofed Route Pointer" and "Fragmented IGMP Packet" Vulnerabilities - Windows 95
9903806	MS99-038,034: "Spoofed Route Pointer" and "Fragmented IGMP Packet" Vulnerabilities - Windows 95 - CORRUPT PATCH
9905201	MS99-052: Legacy Credential Caching Vulnerability in Windows 98
13081125	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2862330 - Windows 7 SP1 (V2.0)
13081127	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2862335 - Windows 7 SP1
13081129	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2864202 - Windows 7 SP1
13081131	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2868038 - Windows 7 SP1
13081137	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2884256 - Windows 7 SP1
13081143	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2862330 - Windows 7 SP1 (x64) (V2.0)
13081145	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2862335 - Windows 7 SP1 (x64)
13081147	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2864202 - Windows 7 SP1 (x64)
13081149	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2868038 - Windows 7 SP1 (x64)
13081155	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2884256 - Windows 7 SP1 (x64)
13081177	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2862330 - Windows 8 Gold
13081179	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2862335 - Windows 8 Gold
13081181	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2863725 - Windows 8 Gold
13081183	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2864202 - Windows 8 Gold
13081185	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2868038 - Windows 8 Gold
13081189	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2884256 - Windows 8 Gold

13081193	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2862330 - Windows 8 Gold (x64)
13081195	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2862335 - Windows 8 Gold (x64)
13081197	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2863725 - Windows 8 Gold (x64)
13081199	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2864202 - Windows 8 Gold (x64)
13081201	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2868038 - Windows 8 Gold (x64)
13081205	MS13-081: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution - KB2884256 - Windows 8 Gold (x64)
14009101	MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege - .NET Framework 4.5.1 - KB2898871 - Windows 8.1 / Windows Server 2012 R2 Gold (x64)
15009102	MS15-009: Security Update for Internet Explorer - Windows 8.1 Gold - IE11 - KB3023607
15065109	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 7 - KB3074886 (x64)
15065110	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 7 - KB3074886 (x64) - CORRUPT PATCH
15065113	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 8 - KB3074886 (x64)
15065114	MS15-065: Security Update for Internet Explorer - Windows Server 2003 SP2 - IE 8 - KB3074886 (x64) - CORRUPT PATCH
81163005	811630: Update for HTML Help Control - Windows NT 4.0
81163009	811630: Update for HTML Help Control - Windows ME
81163010	811630: Update for HTML Help Control - Windows ME - CORRUPT PATCH
82802601	(828026: Update for Windows Media Player Script Commands - WinXP
82802602	828026: Update for Windows Media Player Script Commands - WinME
82802603	828026: Update for Windows Media Player Script Commands - Win NT 4 Server
83235301	(832353: URL Script commands - WinXP
83235303	832353: URL Script commands - WinNT 4.0 Server
87066901	870669 - Disable ADODB.Stream Object From Within Internet Explorer
89112201	891122: An Update for Windows Media Digital Rights Management-enabled players is available - Windows XP
89335701	893357: WPA2/WPS IE Update - Windows XP SP2
89766301	Security Advisory 897663: Windows Firewall Exception May Not Display in the User Interface - Windows XP SP2
89766302	Security Advisory 897663: CORRUPT PATCH - Windows XP SP2

90626701	906267: COM Object (Msdds.dll) Could Cause Internet Explorer to Unexpectedly Exit
91742501	917425: Internet Explorer ActiveX Compatibility Patch for Mshtml.dll - IE 6.0 - Windows XP SP2
91742502	917425: Internet Explorer ActiveX Compatibility Patch for Mshtml.dll - IE 6.0 - Windows XP SP2 - CORRUPT PATCH
91742503	917425: Internet Explorer ActiveX Compatibility Patch for Mshtml.dll - IE 6.0 - Windows Server 2003 SP1
91742504	917425: Internet Explorer ActiveX Compatibility Patch for Mshtml.dll - IE 6.0 - Windows Server 2003 SP1 - CORRUPT PATCH
91742506	917425: Internet Explorer ActiveX Compatibility Patch for Mshtml.dll - IE 6.0 - Windows XP/2003 (x64)
91742507	917425: Internet Explorer ActiveX Compatibility Patch for Mshtml.dll - IE 6.0 - Windows XP/2003 (x64) - CORRUPT PATCH
92572001	925720: Description of the Windows CardSpace hotfix rollup package for Windows XP and Windows Server 2003 - Windows Server 2003 SP1 - KB925720
92572003	925720: Description of the Windows CardSpace hotfix rollup package for Windows XP and Windows Server 2003 - Windows Server 2003 SP1 - KB925720 (x64)
92572005	925720: Description of the Windows CardSpace hotfix rollup package for Windows XP and Windows Server 2003 - Windows XP SP1 - KB925720 (x64)
92572013	925720: Description of the Windows CardSpace hotfix rollup package for Windows XP and Windows Server 2003 - Windows XP SP2 - KB925720
92789107	927891: Fix for Windows Installer - Windows XP (x64)
92789108	927891: Fix for Windows Installer - Windows XP (x64) - CORRUPT PATCH
92789111	927891: Windows Update Agent 3.0 - Windows XP/2003/2000 SP4/Vista/2008 (x86)
92789113	927891: Windows Update Agent 3.0 - Windows XP/2003/Vista/2008 (x64)
92939901	929399: You repeatedly receive a message to install update 929399 on a computer that is running Windows Vista or Windows XP - Windows XP - KB929399
92939903	929399: You repeatedly receive a message to install update 929399 on a computer that is running Windows Vista or Windows XP - Windows Vista - KB929399
92939905	929399: You repeatedly receive a message to install update 929399 on a computer that is running Windows Vista or Windows XP - Windows Vista - KB929399 (x64)
92939907	929399: You repeatedly receive a message to install update 929399 on a computer that is running Windows Vista or Windows XP - Windows XP - KB929399 (x64)

93085701	930857: An update is available for Windows Error Reporting in Windows Vista to make sure that problem reports are sent only after you have granted permission - Windows Vista - KB930857 (x64)
93085703	930857: An update is available for Windows Error Reporting in Windows Vista to make sure that problem reports are sent only after you have granted permission - Windows Vista - KB930857
93259601	932596: Update to Improve Kernel Patch Protection - Windows Vista (x64)
93550901	935509: A software update is available for versions of Windows Vista that include the Windows BitLocker Drive Encryption feature - Windows Vista - KB935509 (x64)
93550903	935509: A software update is available for versions of Windows Vista that include the Windows BitLocker Drive Encryption feature - Windows Vista - KB935509
93635701	936357: A microcode reliability update is available that improves the reliability of systems that use Intel processors - Windows Vista - KB936357
93635703	936357: A microcode reliability update is available that improves the reliability of systems that use Intel processors - Windows Vista - KB936357 (x64)
93635709	936357: A microcode reliability update is available that improves the reliability of systems that use Intel processors - Windows XP SP1 / Windows XP SP2 - KB936357 (x64)
93635719	936357: A microcode reliability update is available that improves the reliability of systems that use Intel processors - Windows XP SP2 - KB936357
93728701	937287: A software update is available for the Windows Vista installation software feature - Windows Vista - KB937287 (x64)
93728703	937287: A software update is available for the Windows Vista installation software feature - Windows Vista - KB937287
93837101	938371: A software update is available for the Windows Vista installation components - Windows Vista - KB938371 (x64)
93837103	938371: A software update is available for the Windows Vista installation components - Windows Vista - KB938371
93915901	939159: An update to prevent a Background Intelligent Transfer Service (BITS) crash on a Windows Vista-based computer - Windows Vista - KB939159 (x64)
93915903	939159: An update to prevent a Background Intelligent Transfer Service (BITS) crash on a Windows Vista-based computer - Windows Vista - KB939159
94015709	940157: Description of Windows Search 4.0 and the Multilingual User Interface Pack for Windows Search 4.0 - Windows XP SP2 (x64)

94015713	940157: Description of Windows Search 4.0 and the Multilingual User Interface Pack for Windows Search 4.0 - Windows Vista SP1 / Windows 2008 Gold (x64)
94015715	940157: Description of Windows Search 4.0 and the Multilingual User Interface Pack for Windows Search 4.0 - Windows Vista SP1 / Windows 2008 Gold
94183301	941833: Update for XML Core Services 4.0 SP2 - Windows Vista
94183303	941833: Update for XML Core Services 4.0 SP2 - Windows Vista (x64)
94341101	943411: Update to Improve Windows Sidebar Protection - Windows Vista
94341103	943411: Update to Improve Windows Sidebar Protection - Windows Vista (x64)
94372907	943729: Information about new Group Policy preferences in Windows 2008 - Windows Vista Gold/SP1/SP2 (x64)
94372909	943729: Information about new Group Policy preferences in Windows 2008 - Windows Vista Gold/SP1/SP2
94372911	943729: Information about new Group Policy preferences in Windows 2008 - Windows XP SP2 (x64)
94662701	946627: Internet Explorer 6 crashes after you install security update 942615 - IE 6 - Windows XP SP2
94993901	949939: Description of a prerequisite software update for Windows Vista update 937287 - Windows Vista - KB949939 (x64)
94993903	949939: Description of a prerequisite software update for Windows Vista update 937287 - Windows Vista - KB949939
95012701	950127: Stop error message when you try to update or to install AVstream device drivers on a Windows Vista-based computer: "Stop error code 0x00000050 (PAGE_FAULT_IN_NONPAGED_AREA)" - Windows Vista - KB950127
95012703	950127: Stop error message when you try to update or to install AVstream device drivers on a Windows Vista-based computer: "Stop error code 0x00000050 (PAGE_FAULT_IN_NONPAGED_AREA)" - Windows Vista - KB950127 (x64)
95161801	951618: A black screen issue occurs on a Windows Vista-based computer or a Windows XP Service Pack 2-based computer that has Onekey Recovery 5.0 installed when you upgrade the operating system - Windows Vista / Windows Vista SP1 - KB951618 (x64)
95161803	951618: A black screen issue occurs on a Windows Vista-based computer or a Windows XP Service Pack 2-based computer that has Onekey Recovery 5.0 installed when you upgrade the operating system - Windows Vista / Windows Vista SP1 - KB951618
95197801	(951978: Script output is not displayed as expected when you run VBScript or JScript scripts in Windows Vista

95197803	951978: Script output is not displayed as expected when you run VBScript or JScript scripts in Windows Vista , in Windows Server 2008, or in Windows XP - Windows Vista SP1 - KB951978 (x64)
95197805	951978: Script output is not displayed as expected when you run VBScript or JScript scripts in Windows Vista , in Windows Server 2008, or in Windows XP - Windows Vista SP1 - KB951978
95197807	(951978: Script output is not displayed as expected when you run VBScript or JScript scripts in Windows Vista
95228701	952287: An application that uses the ADO interface may malfunction, or data loss may occur when the application connects to SQL Server in Windows Vista, in Windows XP, or in Windows Server 2008 - Windows Vista SP1 - KB952287
95228703	(952287: An application that uses the ADO interface may malfunction
95228705	952287: An application that uses the ADO interface may malfunction, or data loss may occur when the application connects to SQL Server in Windows Vista, in Windows XP, or in Windows Server 2008 - Windows Vista SP1 - KB952287 (x64)
95228707	(952287: An application that uses the ADO interface may malfunction
95228711	(952287: An application that uses the ADO interface may malfunction
95270901	952709: A reliability and performance update is available for Windows Vista SP1-based computers - Windows Vista - KB952709 (x64)
95270903	952709: A reliability and performance update is available for Windows Vista SP1-based computers - Windows Vista - KB952709
95383903	953839: Cumulative Security Update for ActiveX - Windows XP SP2/SP3
95383904	953839: Cumulative Security Update for ActiveX - Windows XP SP2/SP3 - CORRUPT PATCH
95383907	953839: Cumulative Security Update for ActiveX - Windows Vista Gold/SP1
95383911	953839: Cumulative Security Update for ActiveX - Windows XP Gold/SP2 (x64)
95383912	953839: Cumulative Security Update for ActiveX - Windows XP Gold/SP2 (x64) - CORRUPT PATCH
95383915	953839: Cumulative Security Update for ActiveX - Windows Vista Gold/SP1 (x64)
95502001	955020: The words "Friendster," "Klum," "Nazr," "Obama," and "Racicot" are not recognized when you check the spelling in Windows Vista and in Windows Server 2008 - Windows Vista / Windows Vista SP1 - KB955020 (x64)
95502003	955020: The words "Friendster," "Klum," "Nazr," "Obama," and "Racicot" are not recognized when you check the spelling in Windows Vista and in Windows Server 2008 - Windows Vista / Windows Vista SP1 - KB955020
95530205	955302: A reliability and performance update is available for computers that are running Windows Vista SP1 and Windows Server 2008 - Windows Vista SP1 - KB955302 (x64)

95530207	955302: A reliability and performance update is available for computers that are running Windows Vista SP1 and Windows Server 2008 - Windows Vista SP1 - KB955302
95543003	955430: Description of the Windows Vista and Windows Server 2008 installation software feature update released April 28, 2009 - Windows Vista Gold/SP1 - KB955430 (x64)
95543007	955430: Description of the Windows Vista and Windows Server 2008 installation software feature update released April 28, 2009 - Windows Vista Gold/SP1 - KB955430
95575907	Security Advisory 955759: AppCompat Update for Indeo Codec - Windows XP SP2 (x64)
95575908	Security Advisory 955759: AppCompat Update for Indeo Codec - Windows XP SP2 (x64) - CORRUPT PATCH
95625002	956250: An update is available for the.NET Framework 3.5 in Windows Vista and in Windows Server 2008 - Windows Server 2008 / Windows Vista - KB956250
95625004	956250: An update is available for the.NET Framework 3.5 in Windows Vista and in Windows Server 2008 - Windows Server 2008 / Windows Vista - KB956250 (x64)
95639103	956391: Cumulative Security Update for ActiveX - Windows XP SP2/SP3
95639104	956391: Cumulative Security Update for ActiveX - Windows XP SP2/SP3 - CORRUPT PATCH
95639107	956391: Cumulative Security Update for ActiveX - Windows Vista Gold/SP1
95639111	956391: Cumulative Security Update for ActiveX - Windows XP Gold/SP2 (x64)
95639112	956391: Cumulative Security Update for ActiveX - Windows XP Gold/SP2 (x64) - CORRUPT PATCH
95639115	956391: Cumulative Security Update for ActiveX - Windows Vista Gold/SP1 (x64)
95782701	957827: Description of the update for Expression Web 2.0 - Expression Web 2 - KB957827
95920921	959209: Update for the .NET Framework 3.5 (May 2009) - Windows Server 2008 / Windows Vista - KB958484
95920923	959209: Update for the .NET Framework 3.5 (May 2009) - Windows Server 2003 Gold / Windows XP Gold - KB958481
95920925	959209: Update for the .NET Framework 3.5 (May 2009) - Windows Server 2008 / Windows Vista - KB958484 (x64)
95920927	959209: Update for the .NET Framework 3.5 (May 2009) - Windows Server 2008 / Windows Vista - KB958481 (x64)
95920929	959209: Update for the .NET Framework 3.5 (May 2009) - Windows Server 2008 / Windows Vista - KB958481
96071521	960715: Update Rollup for ActiveX - Windows XP SP2/SP3

96071522	960715: Update Rollup for ActiveX - Windows XP SP2/SP3 - CORRUPT PATCH
96071525	960715: Update Rollup for ActiveX - Windows Vista Gold/SP1
96071529	960715: Update Rollup for ActiveX - Windows XP Gold/SP2 (x64)
96071530	960715: Update Rollup for ActiveX - Windows XP Gold/SP2 (x64) - CORRUPT PATCH
96071533	960715: Update Rollup for ActiveX - Windows Vista Gold/SP1 (x64)
96370701	963707: How to remove the .NET Framework Assistant for Firefox - Windows Server 2003 / Windows Server 2008 / Windows Vista / Windows XP - KB963707
96370703	963707: How to remove the .NET Framework Assistant for Firefox - Windows Server 2003 / Windows Server 2008 / Windows Vista / Windows XP - KB963707 (x64)
96771509	967715: Update for Windows Autorun - Windows XP Gold (x64)
96771510	967715: Update for Windows Autorun - Windows XP Gold (x64) - CORRUPT PATCH
96790201	967902: You cannot connect to a virtual machine when the Windows Server 2008 Hyper-V VMMS certificate has expired - Windows Server 2008 / Windows Server 2008 / Windows Server 2008 - KB967902 (x64)
96838909	968389: Extended Protection for Authentication - Windows XP SP2 (x64)
96838910	968389: Extended Protection for Authentication - Windows XP SP2 (x64) - CORRUPT PATCH
96873001	968730: Update for Windows XP SP3
96873005	968730: Update for Windows XP SP2 (x64)
96989803	969898: Update Rollup for ActiveX - Windows XP SP2/SP3
96989804	969898: Update Rollup for ActiveX - Windows XP SP2/SP3 - CORRUPT PATCH
96989807	969898: Update Rollup for ActiveX - Windows Vista Gold/SP1/SP2
96989811	969898: Update Rollup for ActiveX - Windows XP Gold/SP2 (x64)
96989812	969898: Update Rollup for ActiveX - Windows XP Gold/SP2 (x64) - CORRUPT PATCH
97043007	970430: Description of the update that implements Extended Protection for Authentication in the HTTP Protocol Stack (http.sys) - Windows XP SP2 - KB970430 (x64)
97043009	970430: Description of the update that implements Extended Protection for Authentication in the HTTP Protocol Stack (http.sys) - Windows Vista - KB970430 (x64)
97043015	970430: Description of the update that implements Extended Protection for Authentication in the HTTP Protocol Stack (http.sys) - Windows XP SP2 / Windows XP SP3 - KB970430
97043019	970430: Description of the update that implements Extended Protection for Authentication in the HTTP Protocol Stack (http.sys) - Windows Vista - KB970430

97102905	971029: Update for Windows Autorun Functionality - Windows Vista Gold/SP1/SP2
97102911	971029: Update for Windows Autorun Functionality - Windows Vista Gold/SP1/SP2 (x64)
97151203	(971512: Windows Graphics
97151207	(971512: Windows Graphics
97289003	Security Advisory 972890: Vulnerability in Microsoft Video ActiveX Control Could Allow Remote Code Execution - Windows XP SP2/SP3
97289007	Security Advisory 972890: Vulnerability in Microsoft Video ActiveX Control Could Allow Remote Code Execution - Windows XP SP2 (x64)
97368601	973686: Update for MSXML Core Services 6.0 Service Pack 2 - Windows XP SP2 (x64)
97368802	973688: Description of an update for Microsoft XML Core Services 4.0 Service Pack 2 - MSXML 4.0 SP2 - KB973688
97647001	976470: The "Date and Time" window shows "Date out of range" error message - Windows Server 2008 SP2 / Windows Vista SP2 - KB976470 (x64)
97647003	976470: The "Date and Time" window shows "Date out of range" error message - Windows Server 2008 SP2 / Windows Vista SP2 - KB976470
97674905	976749: Update for Internet Explorer 6 - Windows XP SP2/SP3
97674906	976749: Update for Internet Explorer 6 - Windows XP SP2/SP3 - CORRUPT PATCH
97674907	976749: Update for Internet Explorer 6 - Windows Server 2003 SP2
97674908	976749: Update for Internet Explorer 6 - Windows Server 2003 SP2 - CORRUPT PATCH
97674909	976749: Update for Internet Explorer 7 - Windows XP SP2/SP3
97674910	976749: Update for Internet Explorer 7 - Windows XP SP2/SP3 - CORRUPT PATCH
97674911	976749: Update for Internet Explorer 7 - Windows Server 2003 SP2
97674913	976749: Update for Internet Explorer 7 - Windows Vista Gold/SP1/SP2
97674914	976749: Update for Internet Explorer 7 - Windows Server 2003 SP2 - CORRUPT PATCH
97674917	976749: Update for Internet Explorer 8 - Windows XP SP2/SP3
97674918	976749: Update for Internet Explorer 8 - Windows XP SP2/SP3 - CORRUPT PATCH
97674919	976749: Update for Internet Explorer 8 - Windows Server 2003 SP2
97674920	976749: Update for Internet Explorer 8 - Windows Server 2003 SP2 - CORRUPT PATCH
97674921	976749: Update for Internet Explorer 8 - Windows Vista Gold/SP1/SP2
97674925	976749: Update for Internet Explorer 8 - Windows 7
97674927	976749: Update for Internet Explorer 6 - Windows XP SP2 (x64)
97674928	976749: Update for Internet Explorer 6 - Windows XP SP2 (x64) - CORRUPT PATCH

97674929	976749: Update for Internet Explorer 6 - Windows Server 2003 SP2 (x64)
97674930	976749: Update for Internet Explorer 6 - Windows Server 2003 SP2 (x64) - CORRUPT PATCH
97674931	976749: Update for Internet Explorer 7 - Windows XP SP2 (x64)
97674932	976749: Update for Internet Explorer 7 - Windows XP SP2 (x64) - CORRUPT PATCH
97674933	976749: Update for Internet Explorer 7 - Windows Server 2003 SP2 (x64)
97674935	976749: Update for Internet Explorer 7 - Windows Vista Gold/SP1/SP2 (x64)
97674936	976749: Update for Internet Explorer 7 - Windows Server 2003 SP2 (x64) - CORRUPT PATCH
97674939	976749: Update for Internet Explorer 8 - Windows XP SP2 (x64)
97674940	976749: Update for Internet Explorer 8 - Windows XP SP2 (x64) - CORRUPT PATCH
97674941	976749: Update for Internet Explorer 8 - Windows Server 2003 SP2 (x64)
97674942	976749: Update for Internet Explorer 8 - Windows Server 2003 SP2 (x64) - CORRUPT PATCH
97674943	976749: Update for Internet Explorer 8 - Windows Vista Gold/SP1/SP2 (x64)
97674946	976749: Update for Internet Explorer 8 - Windows 7 (x64)
97763201	977632: A computer that is running a virtual machine in Windows Virtual PC may stop responding or restart when you resume it from sleep or from hibernation in Windows 7 - Windows 7 - KB977632 (x64)
97763203	977632: A computer that is running a virtual machine in Windows Virtual PC may stop responding or restart when you resume it from sleep or from hibernation in Windows 7 - Windows 7 - KB977632
97909901	979099: An update is available to remove the application manifest expiry feature from AD RMS clients - Windows Server 2008 SP2 - KB979099 (x64)
97909905	979099: An update is available to remove the application manifest expiry feature from AD RMS clients - Windows Server 2008 SP2 - KB979099
97953001	979530: A Windows Server 2008 R2-based Remote Desktop server denies some connection requests randomly under heavy logon or logoff conditions - Windows 7 Gold - KB979530
97953003	979530: A Windows Server 2008 R2-based Remote Desktop server denies some connection requests randomly under heavy logon or logoff conditions - Windows 7 Gold / Windows Server 2008 R2 Gold - KB979530 (x64)
98040801	980408: Update for Windows 7
98040803	980408: Update for Windows 7 (x64)
98201801	982018: An update that improves the compatibility of Windows 7 and Windows Server 2008 R2 with Advanced Format Disks is available - Windows 7 SP1 - KB982018 (x64) (V3.0)

98201805	982018: An update that improves the compatibility of Windows 7 and Windows Server 2008 R2 with Advanced Format Disks is available - Windows 7 SP1 - KB982018 (V3.0)
98252509	982525: An update rollup is available for the .NET Framework 3.5 SP1 in Windows Vista SP2 and in Windows Server 2008 SP2 - Windows Server 2008 SP2 / Windows Vista SP2 - KB956250
98252511	982525: An update rollup is available for the .NET Framework 3.5 SP1 in Windows Vista SP2 and in Windows Server 2008 SP2 - Windows Server 2008 SP2 / Windows Vista SP2 - KB979899 (x64)
98252513	982525: An update rollup is available for the .NET Framework 3.5 SP1 in Windows Vista SP2 and in Windows Server 2008 SP2 - Windows Server 2008 SP2 / Windows Vista SP2 - KB956250 (x64)
98252515	982525: An update rollup is available for the .NET Framework 3.5 SP1 in Windows Vista SP2 and in Windows Server 2008 SP2 - Windows Server 2008 SP2 / Windows Vista SP2 - KB979899
98252601	982526: An update rollup is available for the .NET Framework 3.5 SP1 in Windows 7 and in Windows Server 2008 R2 - Windows 7 - KB958488 (Superseded)
98252603	982526: An update rollup is available for the .NET Framework 3.5 SP1 in Windows 7 and in Windows Server 2008 R2 - Windows 7 / Windows Server 2008 R2 - KB958488 (x64) (Superseded)
98252605	982526: An update rollup is available for the .NET Framework 3.5 SP1 in Windows 7 and in Windows Server 2008 R2 - Windows 7 / Windows Server 2008 R2 - KB979900 (x64) (Superseded)
98252607	982526: An update rollup is available for the .NET Framework 3.5 SP1 in Windows 7 and in Windows Server 2008 R2 - Windows 7 - KB979900 (Superseded)
226571601	2265716: Update for Windows 7
226571603	2265716: Update for Windows 7/2008R2 (x64)
234588604	2345886: Description of the update that implements Extended Protection for Authentication in the Server service - Windows XP SP3 - KB2345886
234588608	2345886: Description of the update that implements Extended Protection for Authentication in the Server service - Windows XP SP2 - KB2345886 (x64)
234588622	2345886: Description of the update that implements Extended Protection for Authentication in the Server service - Windows Vista Gold/SP1 - KB2345886
234588629	2345886: Description of the update that implements Extended Protection for Authentication in the Server service - Windows Vista Gold/SP1 - KB2345886 (x64)
234588631	2345886: Description of the update that implements Extended Protection for Authentication in the Server service - Windows 7 Gold - KB2345886 (x64)

234588633	2345886: Description of the update that implements Extended Protection for Authentication in the Server service - Windows 7 Gold - KB2345886
245094402	(2450944: Some folders or files are unexpectedly deleted on the upstream server after you restart the DFS Replication service in Windows Server 2003 R2
245094404	(2450944: Some folders or files are unexpectedly deleted on the upstream server after you restart the DFS Replication service in Windows Server 2003 R2
245094406	(2450944: Some folders or files are unexpectedly deleted on the upstream server after you restart the DFS Replication service in Windows Server 2003 R2
246887105	2468871: Update for the .NET Framework 4 - Windows XP SP2 / Windows 2003 SP2 / Windows Vista SP2 / Windows 2008 R2 SP1 / Windows 2008 SP2 / Windows 7 Gold/SP1 (x64)
246887109	2468871: Update for the .NET Framework 4 - Windows XP SP3 / Windows 2003 SP2 / Windows Vista SP2 / Windows 2008 SP2 / Windows 7 Gold/SP1
249250501	2492505: Computer does not crash when the disk is full after CrashOnAuditFail is set in Windows 7 or in Windows Server 2008 R2 - Windows 7 Gold/ SP1 / Windows Server 2008 R2 Gold/SP1 - KB2492505 (x64)
249250503	2492505: Computer does not crash when the disk is full after CrashOnAuditFail is set in Windows 7 or in Windows Server 2008 R2 - Windows 7 Gold/SP1 - KB2492505
250518901	2505189: An update is available for DirectWrite and XPS issues in Windows Vista SP2 and in Windows Server 2008 SP2 - Windows Server 2008 SP2 - KB2505189 (x64)
250518907	2505189: An update is available for DirectWrite and XPS issues in Windows Vista SP2 and in Windows Server 2008 SP2 - Windows Server 2008 SP2 - KB2505189
250601401	Security Advisory 2506014: Update for the Windows Operating System Loader - Windows Vista/2008 (x64)
250601403	Security Advisory 2506014: Update for the Windows Operating System Loader - Windows 7/2008R2 (x64)
250614301	Uninstall Windows Management Framework 3.0 - Windows 7 SP1 / Windows Server 2008 R2 SP1 / Windows Server 2012 / Windows 8.1 / Windows Server 2012 R2
250692803	2506928: A link in an .html file that you open in Outlook does not work in Windows 7 or in Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1 (x64)
250692807	2506928: A link in an .html file that you open in Outlook does not work in Windows 7 or in Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1

251532501	2515325: Windows Explorer may crash in Windows 7 or in Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1
251532505	2515325: Windows Explorer may crash in Windows 7 or in Windows Server 2008 R2 - Windows Server 2008 R2 Gold / Windows Server 2008 R2 SP1 (x64)
251532507	2515325: Windows Explorer may crash in Windows 7 or in Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1 (x64)
252015505	2520155: DNS Host record of a computer is deleted after you change the DNS server assignment - Windows Vista SP2 / Windows Server 2008 SP2
253352305	2533523: Reliability Update 1 for the .NET Framework 4 - Windows XP SP2 / Windows 2003 SP2 / Windows Vista SP2 / Windows 2008 R2 Gold/SP1 / Windows 2008 SP2 / Windows 7 Gold/SP1 (x64)
253352309	2533523: Reliability Update 1 for the .NET Framework 4 - Windows XP SP3 / Windows 2003 SP2 / Windows Vista SP2 / Windows 2008 SP2 / Windows 7 Gold/SP1
253362309	2533623: Microsoft Security Advisory: Insecure library loading could allow remote code execution - Windows 7 SP1 - KB2533623 (x64)
253362313	2533623: Microsoft Security Advisory: Insecure library loading could allow remote code execution - Windows 7 SP1 - KB2533623
254569801	2545698: Text in some core fonts appears blurred in Internet Explorer 9 on a computer that is running Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1 (x64)
254569803	(2545698: Text in some core fonts appears blurred in Internet Explorer 9 on a computer that is running Windows Vista
254569805	(2545698: Text in some core fonts appears blurred in Internet Explorer 9 on a computer that is running Windows Vista
254569809	2545698: Text in some core fonts appears blurred in Internet Explorer 9 on a computer that is running Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2 - Windows Vista SP2
254569811	2545698: Text in some core fonts appears blurred in Internet Explorer 9 on a computer that is running Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1
254569815	(2545698: Text in some core fonts appears blurred in Internet Explorer 9 on a computer that is running Windows Vista
254569817	2545698: Text in some core fonts appears blurred in Internet Explorer 9 on a computer that is running Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2 - Windows Vista SP2 (x64)
254766601	2547666: You cannot delete long URLs from the browsing history in Internet Explorer on a computer that is running Windows 7 or Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1 (x64)

254766603	2547666: You cannot delete long URLs from the browsing history in Internet Explorer on a computer that is running Windows 7 or Windows Server 2008 R2 - Windows 2008 R2 Gold / Windows 2008 R2 SP1 (x64)
254766605	2547666: You cannot delete long URLs from the browsing history in Internet Explorer on a computer that is running Windows 7 or Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1
255097801	2550978: "0x0000007B" Stop error after you replace an identical iSCSI network adapter - Windows 7 SP1 - KB2550978
255097803	2550978: "0x0000007B" Stop error after you replace an identical iSCSI network adapter - Windows 7 SP1 - KB2550978 (x64)
255234301	2552343: Time-out error occurs when you install a Windows Update package that contains drivers on a computer that is running Windows 7 or Windows Server 2008 R2 - Windows 7 Gold/SP1
255234305	2552343: Time-out error occurs when you install a Windows Update package that contains drivers on a computer that is running Windows 7 or Windows Server 2008 R2 - Windows 7 Gold/SP1 (x64)
256293701	2562937: Update Rollup for ActiveX - Windows XP SP3
256293705	2562937: Update Rollup for ActiveX - Windows Vista SP2
256293709	2562937: Update Rollup for ActiveX - Windows 7 Gold/SP1
256293711	2562937: Update Rollup for ActiveX - Windows XP SP2 (x64)
256293715	2562937: Update Rollup for ActiveX - Windows Vista SP2 (x64)
256293719	2562937: Update Rollup for ActiveX - Windows 7 Gold/SP1 (x64)
256322701	2563227: An SVG graphic that has attributes that use large values may not be parsed correctly - Windows Vista SP2
256322709	2563227: An SVG graphic that has attributes that use large values may not be parsed correctly - Windows 7 Gold / Windows 7 SP1 (x64)
256322713	2563227: An SVG graphic that has attributes that use large values may not be parsed correctly - Windows Vista SP2 (x64)
256322715	2563227: An SVG graphic that has attributes that use large values may not be parsed correctly - Windows 7 Gold / Windows 7 SP1
257481903	2574819: An update is available that adds support for DTLS in Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1
257481905	2574819: An update is available that adds support for DTLS in Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 (x64)
257815901	2578159: The logon process stops responding in Windows Server 2008 R2 or in Windows 7 - Windows 7 Gold/SP1 - KB2578159
257815903	2578159: The logon process stops responding in Windows Server 2008 R2 or in Windows 7 - Windows 7 Gold/SP1 / Windows Server 2008 R2 Gold/SP1 - KB2578159 (x64)
259268701	2592687: Remote Desktop Protocol (RDP) 8.0 update for Windows 7 and Windows Server 2008 R2 - Windows 7 SP1
259268703	2592687: Remote Desktop Protocol (RDP) 8.0 update for Windows 7 and Windows Server 2008 R2 - Windows 7 SP1 (x64)

260021703	2600217: Reliability Update 2 for the .NET Framework 4 - Windows XP SP3 / Windows 2003 SP2 / Windows Vista SP2 / Windows 2008 SP2 / Windows 7 Gold/SP1
260021709	2600217: Reliability Update 2 for the .NET Framework 4 - Windows XP SP2 / Windows 2003 SP2 / Windows Vista SP2 / Windows 2008 R2 Gold/SP1 / Windows 2008 SP2 / Windows 7 Gold/SP1 (x64)
261785801	2617858: Unexpectedly slow startup or logon process in Windows Server 2008 R2 or in Windows 7 - Windows 7 SP1
261785803	2617858: Unexpectedly slow startup or logon process in Windows Server 2008 R2 or in Windows 7 - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)
263751801	2637518: An update is available - .NET Framework 3.5.1 - Windows 7 Gold
263751803	2637518: An update is available - .NET Framework 3.5.1 - Windows 7 SP1
263751805	2637518: An update is available - .NET Framework 3.5.1 - Windows Vista SP2 / Windows 2008 SP2 (x64)
263751807	2637518: An update is available - .NET Framework 3.5.1 - Windows 2008 R2 Gold / Windows 7 Gold (x64)
263751809	2637518: An update is available - .NET Framework 3.5.1 - Windows 2008 R2 SP1 / Windows 7 SP1 (x64) (Superseded)
263751811	2637518: An update is available - .NET Framework 3.5.1 - Windows Vista SP2 / Windows 2008 SP2
264014801	2640148: Windows Explorer stops responding if you try to expand a mapped drive in Windows 7 or in Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1 (x64)
264014803	2640148: Windows Explorer stops responding if you try to expand a mapped drive in Windows 7 or in Windows Server 2008 R2 - Windows Server 2008 R2 Gold / Windows Server 2008 R2 SP1 (x64)
264014805	2640148: Windows Explorer stops responding if you try to expand a mapped drive in Windows 7 or in Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1
264656301	2646563: SMB2 directory cache is not updated correctly if a file is deleted in Windows 7 or in Windows Server 2008 R2 - Windows 7 SP1
264656303	2646563: SMB2 directory cache is not updated correctly if a file is deleted in Windows 7 or in Windows Server 2008 R2 - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)
264775303	2647753: Update rollup: Fix printing problems in Windows 7 and Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1
264775307	2647753: Update rollup: Fix printing problems in Windows 7 and Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1 (x64)
266007501	2660075: You cannot change the time and date if the time zone is set to Samoa (UTC+13:00) and KB 2657025 is installed in Windows 7 or in Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1

266007507	2660075: You cannot change the time and date if the time zone is set to Samoa (UTC+13:00) and KB 2657025 is installed in Windows 7 or in Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1 (x64)
267083801	2670838: A platform update is available for Windows 7 SP1 and Windows 2008 R2 SP1 - Windows 7 SP1
267083803	2670838: A platform update is available for Windows 7 SP1 and Windows 2008 R2 SP1 - Windows 2008 R2 SP1 / Windows 7 SP1 (x64)
268581301	2685813: User-Mode Driver Framework version 1.11 update for Windows 7 and Windows Server 2008 R2 - Windows 7 Gold
268581303	2685813: User-Mode Driver Framework version 1.11 update for Windows 7 and Windows Server 2008 R2 - Windows 7 Gold / Windows Server 2008 R2 Gold (x64)
270963003	2709630: Delay occurs when you log on to a domain from a computer that is running Windows 7 or Windows Server 2008 R2 - Windows 7 Gold (x64)
270963007	2709630: Delay occurs when you log on to a domain from a computer that is running Windows 7 or Windows Server 2008 R2 - Windows 7 Gold
271312801	2713128: A network printer is displayed incorrectly as offline on a computer that is running Windows 7 or Windows Server 2008 R2 - Windows 7 Gold/SP1
271312803	2713128: A network printer is displayed incorrectly as offline on a computer that is running Windows 7 or Windows Server 2008 R2 - Windows 7 Gold/SP1 / Windows 2008 R2 Gold/SP1 (x64)
271869505	2718695: Internet Explorer 10 Available - Prerequisites - Windows 7 SP1
271870409	2718704: Unauthorized Digital Certificates Could Allow Spoofing - Windows Vista SP2
271870411	2718704: Unauthorized Digital Certificates Could Allow Spoofing - Windows Vista SP2 (x64)
271966201	2719662: Vulnerabilities in Gadgets Could Allow Remote Code Execution - Disable Windows Sidebar and Gadgets - Windows Vista SP1/SP2 / 7 Gold/SP1
271966203	2719662: Vulnerabilities in Gadgets Could Allow Remote Code Execution - Enable Windows Sidebar and Gadgets - Windows Vista SP1/SP2 / 7 Gold/SP1
272653501	2726535: An update is available that adds South Sudan to the list of countries in Windows Server 2008, Windows 7, and Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1
272653505	2726535: An update is available that adds South Sudan to the list of countries in Windows Server 2008, Windows 7, and Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1 (x64)
272873801	2728738: You experience a long logon time when you try to log on to a Windows 7-based or a Windows Server 2008 R2-based client computer that uses roaming profiles - Windows 7 SP1

272873803	2728738: You experience a long logon time when you try to log on to a Windows 7-based or a Windows Server 2008 R2-based client computer that uses roaming profiles - Windows 7 SP1 / Windows 2008 R2 SP1 (x64)
272909403	2729094: An update for the Segoe UI symbol font in Windows 7 and in Windows 2008 R2 is available - Windows 7 Gold/SP1 (x64)
272909405	2729094: An update for the Segoe UI symbol font in Windows 7 and in Windows 2008 R2 is available - Windows 7 Gold/SP1
273250001	2732500: "E_UNEXPECTED 0x8000ffff" error when you try to restore a system by using System Recovery Options in Windows 7 - Windows 7 Gold (x64)
273250003	2732500: "E_UNEXPECTED 0x8000ffff" error when you try to restore a system by using System Recovery Options in Windows 7 - Windows 7 Gold
273267305	2732673:"Delayed write failed" error message when .pst files are stored on a network file server that is running Windows 7 SP1 /Windows Server 2008 R2 SP1 (x64)
273267307	2732673:"Delayed write failed" error message when .pst files are stored on a network file server that is running Windows 7 SP1
273464201	2734642: RDS-based applications crash in Windows 7 SP1 or Windows Server 2008 R2 SP1 - Windows 7 SP1
273464203	2734642: RDS-based applications crash in Windows 7 SP1 or Windows Server 2008 R2 SP1 - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)
273687801	2736878: 802.1X authentication fails after you connect a computer to a network in Windows 7 SP1 or Windows Server 2008 R2 SP1 - Windows 7 SP1 (x64)
273687803	2736878: 802.1X authentication fails after you connect a computer to a network in Windows 7 SP1 or Windows Server 2008 R2 SP1 - Windows 7 SP1
274824607	2748246: "The Specified port is unknown" error message when you use GPP to deploy printers to a computer that is running Windows - Windows Vista SP2 / Windows Server 2008 SP2 (x64)
274834901	2748349: An update is available - Windows Vista SP2 (x64)
274834907	2748349: An update is available - Windows Vista SP2
274834909	2748349: An update is available - Windows 7 Gold
274834913	2748349: An update is available - Windows 7 Gold (x64)
275014701	2750147: An update is available for the .NET Framework 4.5 - Windows 7 SP1 / Windows 2008 SP2 / Windows Vista SP2
275014703	2750147: An update is available for the .NET Framework 4.5 - Windows 7 SP1 / Windows 2008 SP2 / Windows 2008 R2 SP1 / Windows Vista SP2 (x64)
275014901	2750149: An update is available for the .NET Framework 4.5 in Windows 8, Windows RT and Windows Server 2012 - Windows 8 Gold

275014905	2750149: An update is available for the .NET Framework 4.5 in Windows 8, Windows RT and Windows Server 2012 - Windows 8 Gold / Windows Server 2012 Gold (x64)
275084103	2750841: An IPv6 readiness update is available for Windows 7 and for Windows Server 2008 R2 - Windows 7 SP1
275084105	2750841: An IPv6 readiness update is available for Windows 7 and for Windows Server 2008 R2 - Windows 7 SP1 (x64)
276121703	2761217: An update is available to add the Calibri Light and Calibri Light Italic fonts to Windows 7 and Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1 (x64)
276121705	2761217: An update is available to add the Calibri Light and Calibri Light Italic fonts to Windows 7 and Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1
276367407	2763674: You cannot run an application that is signed with a SHA-256 certificate on a computer that is running Windows Vista SP2 or Windows Server 2008 SP2 - Windows Vista SP2 (x64)
276367409	2763674: You cannot run an application that is signed with a SHA-256 certificate on a computer that is running Windows Vista SP2 or Windows Server 2008 SP2 - Windows Vista SP2
276903403	2769034: WinRE is not enabled after you run the OOBE wizard in Windows 8, Windows RT, or Windows Server 2012 - Windows 8 - KB2769034 (x64)
276903405	2769034: WinRE is not enabled after you run the OOBE wizard in Windows 8, Windows RT, or Windows Server 2012 - Windows 8 - KB2769034
276916501	2769165: An update is available for certain Microsoft files that contain an incorrect digital signature in Windows 8 and Windows 2012 - Windows 8 Gold
276916505	2769165: An update is available for certain Microsoft files that contain an incorrect digital signature in Windows 8 and Windows 2012 - Windows 8 Gold (x64)
277081605	2770816: Windows Update stops at 13 percent in Windows 8 or Windows Server 2012 - Windows 8 - KB2770816 (x64)
277081607	2770816: Windows Update stops at 13 percent in Windows 8 or Windows Server 2012 - Windows 8 - KB2770816
277091701	2770917: Windows 8 and Windows 2012 cumulative update: November 2012 - Windows 8 Gold (KB2771821) (x64)
277091703	2770917: Windows 8 and Windows 2012 cumulative update: November 2012 - Windows 8 Gold (KB2777166)
277091707	2770917: Windows 8 and Windows 2012 cumulative update: November 2012 - Windows 8 Gold (KB2771744) (x64)
277091709	2770917: Windows 8 and Windows 2012 cumulative update: November 2012 - Windows 8 Gold (KB2780342)

277091713	2770917: Windows 8 and Windows 2012 cumulative update: November 2012 - Windows 8 Gold (KB2771821)
277091715	2770917: Windows 8 and Windows 2012 cumulative update: November 2012 - Windows 8 Gold (KB2758246) (x64)
277091717	2770917: Windows 8 and Windows 2012 cumulative update: November 2012 - Windows 8 Gold (KB2771744)
277091719	2770917: Windows 8 and Windows 2012 cumulative update: November 2012 - Windows 8 Gold (KB2758246)
277091721	2770917: Windows 8 and Windows 2012 cumulative update: November 2012 - Windows 8 Gold (KB2780523) (x64)
277091723	2770917: Windows 8 and Windows 2012 cumulative update: November 2012 - Windows 8 Gold (KB2778171) (x64)
277091725	2770917: Windows 8 and Windows 2012 cumulative update: November 2012 - Windows 8 Gold (x64)
277091729	2770917: Windows 8 and Windows 2012 cumulative update: November 2012 - Windows 8 Gold (KB2780523)
277091733	2770917: Windows 8 and Windows 2012 cumulative update: November 2012 - Windows 8 Gold (KB2778171)
277091735	2770917: Windows 8 and Windows 2012 cumulative update: November 2012 - Windows 8 Gold
277091739	2770917: Windows 8 and Windows 2012 cumulative update: November 2012 - Windows 8 Gold (KB2777166) (x64)
277091747	2770917: Windows 8 and Windows 2012 cumulative update: November 2012 - Windows 8 Gold (KB2780342) (x64)
277976801	2779768: Windows 8 and Windows Server 2012 update rollup: December 2012 - Windows 8 Gold (x64) (KB2779768)
277976803	2779768: Windows 8 and Windows Server 2012 update rollup: December 2012 - Windows 8 Gold (x64) (KB2782419)
277976805	2779768: Windows 8 and Windows Server 2012 update rollup: December 2012 - Windows 8 Gold (x64) (KB2783251)
277976807	2779768: Windows 8 and Windows Server 2012 update rollup: December 2012 - Windows 8 Gold (x64) (KB2784160)
277976809	2779768: Windows 8 and Windows Server 2012 update rollup: December 2012 - Windows 8 Gold (KB2779768)
277976811	2779768: Windows 8 and Windows Server 2012 update rollup: December 2012 - Windows 8 Gold (KB2782419)
277976813	2779768: Windows 8 and Windows Server 2012 update rollup: December 2012 - Windows 8 Gold (KB2783251)
277976815	2779768: Windows 8 and Windows Server 2012 update rollup: December 2012 - Windows 8 Gold (KB2784160)
277976817	2779768: Windows 8 and Windows Server 2012 update rollup: December 2012 - Windows 8 Gold (KB2788261)

278509403	2785094: Windows 8 and Windows 2012 cumulative update: January 2013 - Windows 8 Gold (KB2788350)
278509405	2785094: Windows 8 and Windows 2012 cumulative update: January 2013 - Windows 8 Gold (KB2785094) (x64)
278509407	2785094: Windows 8 and Windows 2012 cumulative update: January 2013 - Windows 8 Gold (KB2790920) (x64)
278509409	2785094: Windows 8 and Windows 2012 cumulative update: January 2013 - Windows 8 Gold (KB2792009) (x64)
278509415	2785094: Windows 8 and Windows 2012 cumulative update: January 2013 - Windows 8 Gold (KB2785094)
278509417	2785094: Windows 8 and Windows 2012 cumulative update: January 2013 - Windows 8 Gold (KB2790920)
278509419	2785094: Windows 8 and Windows 2012 cumulative update: January 2013 - Windows 8 Gold (KB2788350) (x64)
278509423	2785094: Windows 8 and Windows 2012 cumulative update: January 2013 - Windows 8 Gold (KB2792009)
278608101	2786081: Internet Explorer 10 does not save credentials for a website after you log off or restart a computer that is running Windows 7 SP1 or Windows 2008 R2 SP1 - Windows 2008 R2 SP1 (x64)
278608103	2786081: Internet Explorer 10 does not save credentials for a website after you log off or restart a computer that is running Windows 7 SP1 or Windows 2008 R2 SP1 - Windows 7 SP1 (x64)
278608105	2786081: Internet Explorer 10 does not save credentials for a website after you log off or restart a computer that is running Windows 7 SP1 or Windows 2008 R2 SP1 - Windows 7 SP1
278640003	2786400: An update is available that changes the default settings of the shaping behavior for Arabic text rendering in Windows 7 and Windows Server 2008 R2 - Windows 7 Gold
278640007	2786400: An update is available that changes the default settings of the shaping behavior for Arabic text rendering in Windows 7 and Windows Server 2008 R2 - Windows 7 Gold (x64)
279594401	2795944: Windows 8 and Windows 2012 cumulative update: February 2013 - Windows 8 Gold (KB2803676) (x64)
279594403	2795944: Windows 8 and Windows 2012 cumulative update: February 2013 - Windows 8 Gold (x64)
279594409	2795944: Windows 8 and Windows 2012 cumulative update: February 2013 - Windows 8 Gold (KB2803676)
279594411	2795944: Windows 8 and Windows 2012 cumulative update: February 2013 - Windows 8 Gold
279599303	2795993: New Share Wizard does not start when you try to create a cluster file share on a third-party dynamic disk resource in Windows 8 or Windows Server 2012 - Windows 8 Gold (x64)

279599305	2795993: New Share Wizard does not start when you try to create a cluster file share on a third-party dynamic disk resource in Windows 8 or Windows Server 2012 - Windows 8 Gold
279599703	2795997: UI is displayed incorrectly when you right-click a third-party dynamic disk resource in the Available Storage area in Windows Server 2012 - Windows 8 Gold (x64)
279599705	2795997: UI is displayed incorrectly when you right-click a third-party dynamic disk resource in the Available Storage area in Windows Server 2012 - Windows 8 Gold
279600003	2796000: You cannot create a cluster file share on a third-party dynamic disk resource in Windows Server 2012 - Windows 8 Gold (x64)
279600005	2796000: You cannot create a cluster file share on a third-party dynamic disk resource in Windows Server 2012 - Windows 8 Gold
279816201	2798162: Update to improve messaging in dialog boxes when you run executable files in Windows - Windows 8 Gold
279816203	2798162: Update to improve messaging in dialog boxes when you run executable files in Windows - Windows 8 Gold (x64)
279992603	2799926: USB storage device cannot be recognized or mounted on a computer that is running Windows 7 or Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1 (x64)
279992607	2799926: USB storage device cannot be recognized or mounted on a computer that is running Windows 7 or Windows Server 2008 R2 - Windows 7 Gold / Windows 7 SP1
280003301	2800033: Windows cannot be restored on a Windows RT-based, Windows 8-based or Windows Server 2012-based computer - Windows 8 Gold (x64)
280003303	2800033: Windows cannot be restored on a Windows RT-based, Windows 8-based or Windows Server 2012-based computer - Windows 8 Gold
280261801	2802618: Invalid TxR log files are generated every time that a registry hive is loaded in Windows 8 or Windows Server 2012 - Windows 8 Gold (x64)
280261805	2802618: Invalid TxR log files are generated every time that a registry hive is loaded in Windows 8 or Windows Server 2012 - Windows 8 Gold
280374801	2803748: Failover Cluster Management snap-in crashes after you install update 2750149 on a Windows 2012-based failover cluster - Windows 8 Gold
280374805	2803748: Failover Cluster Management snap-in crashes after you install update 2750149 on a Windows 2012-based failover cluster - Windows 8 Gold (x64)
280522103	2805221: An update is available for the .NET Framework 4.5 - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2

280522105	2805221: An update is available for the .NET Framework 4.5 - Windows 7 SP1 / Windows Server 2008 R2 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 (x64)
280522601	2805226: An update is available for the .NET Framework 4.5 - Windows 7 SP1 / Windows Server 2008 SP2 / Windows Vista SP2
280522603	2805226: An update is available for the .NET Framework 4.5 - Windows 7 SP1 / Windows Server 2008 R2 SP1 / Windows Server 2008 SP2 / Windows Vista SP2 (x64)
280522701	2805227: An update is available for the .NET Framework 4.5 in Windows 8, Windows RT, and Windows Server 2012 - Windows 8 Gold
280522705	2805227: An update is available for the .NET Framework 4.5 in Windows 8, Windows RT, and Windows Server 2012 - Windows 8 Gold / Windows Server 2012 Gold (x64)
280596601	2805966: Temporary Internet files and history are lost in Internet Explorer 10 after you upgrade from Windows 7 or Windows Server 2008 R2 to Windows 8 or Windows Server 2012 - Windows 8 Gold
280596603	2805966: Temporary Internet files and history are lost in Internet Explorer 10 after you upgrade from Windows 7 or Windows Server 2008 R2 to Windows 8 or Windows Server 2012 - Windows 2012 Gold (x64)
280596605	2805966: Temporary Internet files and history are lost in Internet Explorer 10 after you upgrade from Windows 7 or Windows Server 2008 R2 to Windows 8 or Windows Server 2012 - Windows 8 Gold (x64)
280867901	2808679: Update that protects from internal URL port scanning is available - Windows 8 Gold (x64)
280867907	2808679: Update that protects from internal URL port scanning is available - Windows Vista SP2
280867913	2808679: Update that protects from internal URL port scanning is available - Windows 8 Gold
280867917	2808679: Update that protects from internal URL port scanning is available - Windows 7 SP1
280867921	2808679: Update that protects from internal URL port scanning is available - Windows XP SP2 (x64)
280867927	2808679: Update that protects from internal URL port scanning is available - Windows 7 SP1 (x64)
280867929	2808679: Update that protects from internal URL port scanning is available - Windows Vista SP2 (x64)
281166003	2811660: Windows 8 and Windows 2012 cumulative update: March 2013 - Windows 8 Gold (KB2815769)
281166005	2811660: Windows 8 and Windows 2012 cumulative update: March 2013 - Windows 8 Gold (KB2823233)
281166007	2811660: Windows 8 and Windows 2012 cumulative update: March 2013 - Windows 8 Gold (KB2800088) (x64)

281166009	2811660: Windows 8 and Windows 2012 cumulative update: March 2013 - Windows 8 Gold (KB2812829)
281166011	2811660: Windows 8 and Windows 2012 cumulative update: March 2013 - Windows 8 Gold (KB2812829) (x64)
281166015	2811660: Windows 8 and Windows 2012 cumulative update: March 2013 - Windows 8 Gold (KB2800088)
281166017	2811660: Windows 8 and Windows 2012 cumulative update: March 2013 - Windows 8 Gold (x64)
281166023	2811660: Windows 8 and Windows 2012 cumulative update: March 2013 - Windows 8 Gold
281166025	2811660: Windows 8 and Windows 2012 cumulative update: March 2013 - Windows 8 Gold (KB2815769) (x64)
281166027	2811660: Windows 8 and Windows 2012 cumulative update: March 2013 - Windows 8 Gold (KB2823233) (x64)
281343001	2813430: An update is available that enables administrators to update trusted and disallowed CTLs in disconnected environments in Windows - Windows Vista SP2
281343005	2813430: An update is available that enables administrators to update trusted and disallowed CTLs in disconnected environments in Windows - Windows 7 SP1
281343007	2813430: An update is available that enables administrators to update trusted and disallowed CTLs in disconnected environments in Windows - Windows 8 Gold
281343009	2813430: An update is available that enables administrators to update trusted and disallowed CTLs in disconnected environments in Windows - Windows Vista SP2 (x64)
281343013	2813430: An update is available that enables administrators to update trusted and disallowed CTLs in disconnected environments in Windows - Windows 7 SP1 (x64)
281343017	2813430: An update is available that enables administrators to update trusted and disallowed CTLs in disconnected environments in Windows - Windows 8 Gold (x64)
281860401	2818604: A microcode update is available for Windows 8-based computers that use AMD processors - Windows 8 Gold (x64)
282019709	2820197: Update Rollup for ActiveX Kill Bits - Windows 7 Gold/SP1
282019721	2820197: Update Rollup for ActiveX Kill Bits - Windows 7 Gold/SP1 (x64)
282033101	2820331: Application compatibility update for Windows 7 and Windows Server 2008 R2 - Windows 7 SP1
282033105	2820331: Application compatibility update for Windows 7 and Windows Server 2008 R2 - Windows 7 SP1 (x64)
282224105	2822241: Windows 8 and Windows 2012 cumulative update: April 2013 - Windows 8 Gold (KB2823516)

282224107	2822241: Windows 8 and Windows 2012 cumulative update: April 2013 - Windows 8 Gold (x64) (KB2823516)
282224109	2822241: Windows 8 and Windows 2012 cumulative update: April 2013 - Windows 8 Gold
282224111	2822241: Windows 8 and Windows 2012 cumulative update: April 2013 - Windows 8 Gold (x64)
282318007	2823180: Update is available for Windows Management Framework 3.0 in Windows 7 SP1, Windows Server 2008 R2 SP1, or Windows Server 2008 SP2 - KB2823180 - Windows 7 SP1 (x64)
282318009	2823180: Update is available for Windows Management Framework 3.0 in Windows 7 SP1, Windows Server 2008 R2 SP1, or Windows Server 2008 SP2 - KB2809215 - Windows 7 SP1 (x64)
282318011	2823180: Update is available for Windows Management Framework 3.0 in Windows 7 SP1, Windows Server 2008 R2 SP1, or Windows Server 2008 SP2 - KB2809900 - Windows 7 SP1 (x64)
282318017	2823180: Update is available for Windows Management Framework 3.0 in Windows 7 SP1, Windows Server 2008 R2 SP1, or Windows Server 2008 SP2 - KB2823180 - Windows 7 SP1
282318019	2823180: Update is available for Windows Management Framework 3.0 in Windows 7 SP1, Windows Server 2008 R2 SP1, or Windows Server 2008 SP2 - KB2809900 - Windows 7 SP1
283047701	2830477: Update for RemoteApp and Desktop Connections feature is available for Windows - KB2574819 - Windows 7 SP1
283047703	2830477: Update for RemoteApp and Desktop Connections feature is available for Windows - KB2830477 - Windows 7 SP1
283047705	2830477: Update for RemoteApp and Desktop Connections feature is available for Windows - KB2857650 - Windows 7 SP1
283047717	2830477: Update for RemoteApp and Desktop Connections feature is available for Windows - KB2574819 - Windows 7 SP1 (x64)
283047719	2830477: Update for RemoteApp and Desktop Connections feature is available for Windows - KB2830477 - Windows 7 SP1 (x64)
283047721	2830477: Update for RemoteApp and Desktop Connections feature is available for Windows - KB2857650 - Windows 7 SP1 (x64)
283414007	2834140: "0x00000050" Stop error after you install update 2670838 on a computer that is running Windows 7 SP1 or Windows Server 2008 R2 SP1 - Windows 7 SP1
283414009	2834140: "0x00000050" Stop error after you install update 2670838 on a computer that is running Windows 7 SP1 or Windows Server 2008 R2 SP1 - Windows 7 SP1 (x64)
283517403	2835174: Incorrect disclaimer is displayed in the Product Activation wizard in the Polish version of Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1

283517405	2835174: Incorrect disclaimer is displayed in the Product Activation wizard in the Polish version of Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 (x64)
283693911	2836939: An update is available - .Net Framework 4.0 - Windows 7 SP1 / 2008 R2 SP1 / 2008 SP2 / Vista SP2 / 2003 SP2 / XP SP2 (x64)
283693913	2836939: An update is available - .Net Framework 4.0 - Windows 7 SP1 / 2008 SP2 / Vista SP2 / 2003 SP2 / XP SP3
283694011	2836940: An update is available for the .NET Framework 3.5 SP1 - Windows Server 2003 SP2 / Windows Server 2008 SP2 / Windows Vista SP2 / Windows XP SP3
283694013	2836940: An update is available for the .NET Framework 3.5 SP1 - Windows Server 2003 SP2 / Windows Server 2008 SP2 / Windows Vista SP2 / Windows XP SP2 (x64)
283694111	2836941: An update is available for the .NET Framework 2.0 SP2 on Windows XP and Windows Server 2003 - Windows XP SP2 / 2003 SP2 (x64)
283694113	2836941: An update is available for the .NET Framework 2.0 SP2 on Windows XP and Windows Server 2003 - Windows XP SP3 / 2003 SP2
283694201	2836942: Update for the .NET Framework 3.5.1 on Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1
283694203	2836942: Update for the .NET Framework 3.5.1 on Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)
283694301	2836943: An update is available for the .NET Framework 3.5.1- Windows 7 SP1 / Windows 2008 R2 SP1 (x64)
283694303	2836943: An update is available for the .NET Framework 3.5.1- Windows 7 SP1
283694601	2836946: An update is available for the .NET Framework 3.5 on Windows 8 and Windows Server 2012 - Windows 8 Gold / Windows Server 2012 Gold (x64)
283694603	2836946: An update is available for the .NET Framework 3.5 on Windows 8 and Windows Server 2012 - Windows 8 Gold
283694701	2836947: An update is available for the .NET Framework 3.5 on Windows 8 and Windows Server 2012 - Windows 8 Gold
283694703	2836947: An update is available for the .NET Framework 3.5 on Windows 8 and Windows Server 2012 - Windows 8 Gold / Windows Server 2012 Gold (x64)
283698801	2836988: Windows 8 and Windows Server 2012 update rollup - Windows 8 Gold (x64)
283698803	2836988: Windows 8 and Windows Server 2012 update rollup - Windows 8 Gold
284113401	2841134: Internet Explorer 11 Available - Install - Windows 7 SP1
284113403	2841134: Internet Explorer 11 Available - Install - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)

284113407	2841134: Internet Explorer 11 Available - Prerequisites - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)
284223003	2842230: "Out of memory" error on a computer that has a customized MaxMemoryPerShellMB quota set and has WMF 3.0 installed - Windows 8 - KB2842230 (x64)
284223005	2842230: "Out of memory" error on a computer that has a customized MaxMemoryPerShellMB quota set and has WMF 3.0 installed - Windows 8 - KB2842230
284223007	2842230: "Out of memory" error on a computer that has a customized MaxMemoryPerShellMB quota set and has WMF 3.0 installed - Windows 7 SP1 - KB2842230 (x64)
284223009	2842230: "Out of memory" error on a computer that has a customized MaxMemoryPerShellMB quota set and has WMF 3.0 installed - Windows 7 SP1 - KB2842230
284223011	2842230: "Out of memory" error on a computer that has a customized MaxMemoryPerShellMB quota set and has WMF 3.0 installed - Windows Vista SP2 - KB2842230
284223013	2842230: "Out of memory" error on a computer that has a customized MaxMemoryPerShellMB quota set and has WMF 3.0 installed - Windows Vista SP2 - KB2842230 (x64)
284553309	2845533: Windows RT, Windows 8, and Windows Server 2012 update rollup: June 2013 - Windows 8 Gold
284553311	2845533: Windows RT, Windows 8, and Windows Server 2012 update rollup: June 2013 - Windows 8 Gold
284553313	2845533: Windows RT, Windows 8, and Windows Server 2012 update rollup: June 2013 - Windows 8 Gold
284553315	2845533: Windows RT, Windows 8, and Windows Server 2012 update rollup: June 2013 - Windows 8 Gold
284553317	2845533: Windows RT, Windows 8, and Windows Server 2012 update rollup: June 2013 - Windows 8 Gold (x64)
284553319	2845533: Windows RT, Windows 8, and Windows Server 2012 update rollup: June 2013 - Windows 8 Gold (x64) (KB2850674)
284553321	2845533: Windows RT, Windows 8, and Windows Server 2012 update rollup: June 2013 - Windows 8 Gold (x64) (KB2853915)
284553323	2845533: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold (x64) (KB2856758)
285238601	2852386: Disk Cleanup Wizard addon lets users delete outdated Windows updates on Windows 7 SP1 or Windows Server 2008 R2 SP1 - Windows 7 SP1
285238603	2852386: Disk Cleanup Wizard addon lets users delete outdated Windows updates on Windows 7 SP1 or Windows Server 2008 R2 SP1 - Windows 7 SP1 (x64)

285395201	2853952: Loss of consistency with IDE-attached virtual hard disks when a Hyper-V host server experiences an unplanned restart - Windows 7 SP1 - KB2853952
285395203	2853952: Loss of consistency with IDE-attached virtual hard disks when a Hyper-V host server experiences an unplanned restart - Windows 7 SP1 - KB2853952 (x64)
285395205	2853952: Loss of consistency with IDE-attached virtual hard disks when a Hyper-V host server experiences an unplanned restart - Windows Server 2008 R2 SP1 - KB2853952 (x64)
285533607	2855336: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold (x64) (KB2855336)
285533609	2855336: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold (KB2855336)
285872501	2858725: Microsoft .NET Framework 4.5.1 Available - Windows 7 SP1 / Windows 8 Gold / Windows 2008 R2 SP1 / Windows 2008 SP2 / Windows 2012 Gold / Windows Vista SP2 (x64)
285872503	2858725: Microsoft .NET Framework 4.5.1 Available - Windows 7 SP1 / Windows 8 Gold / Windows 2008 SP2 / Windows Vista SP2
286185513	2861855: Updates to improve Remote Desktop Protocol network-level authentication - Windows Vista SP2 (x64)
286185517	2861855: Updates to improve Remote Desktop Protocol network-level authentication - Windows Vista SP2
286215203	2862152: Microsoft security advisory: Vulnerability in DirectAccess could allow security feature bypass - Windows Vista SP2
286215205	2862152: Microsoft security advisory: Vulnerability in DirectAccess could allow security feature bypass - Windows 8 Gold (x64)
286215211	2862152: Microsoft security advisory: Vulnerability in DirectAccess could allow security feature bypass - Windows 7 SP1 (x64)
286215217	2862152: Microsoft security advisory: Vulnerability in DirectAccess could allow security feature bypass - Windows XP SP2 (x64)
286215233	2862152: Microsoft security advisory: Vulnerability in DirectAccess could allow security feature bypass - Windows 8 Gold
286215235	2862152: Microsoft security advisory: Vulnerability in DirectAccess could allow security feature bypass - Windows Vista SP2 (x64)
286215237	2862152: Microsoft security advisory: Vulnerability in DirectAccess could allow security feature bypass - Windows 7 SP1
286276803	2862768: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold
286276805	2862768: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold (x64)
286296605	2862966: An update is available that improves management of weak certificate cryptographic algorithms in Windows - Windows Vista SP2 (x64)

286296611	2862966: An update is available that improves management of weak certificate cryptographic algorithms in Windows - Windows Vista SP2
286296613	2862966: An update is available that improves management of weak certificate cryptographic algorithms in Windows - Windows 8 Gold (x64)
286296621	2862966: An update is available that improves management of weak certificate cryptographic algorithms in Windows - Windows 8 Gold
286297303	2862973: Update for deprecation of MD5 hashing algorithm for Microsoft root certificate program - Windows Vista SP2 (x64)
286297307	2862973: Update for deprecation of MD5 hashing algorithm for Microsoft root certificate program - Windows Vista SP2
287138901	2871389: Update is available that prepares Windows 8 and Windows RT-based computers for the update to Windows 8.1 and Windows 8.1 RT - Windows 8 Gold
287138905	2871389: Update is available that prepares Windows 8 and Windows RT-based computers for the update to Windows 8.1 and Windows 8.1 RT - Windows 8 Gold (x64)
287199709	2871997: Security Advisory: Update to fix the Pass-The-Hash Vulnerability - Windows 8 Gold (x64)
287199713	2871997: Security Advisory: Update to fix the Pass-The-Hash Vulnerability - Windows 7 SP1 (x64)
287199715	2871997: Security Advisory: Update to fix the Pass-The-Hash Vulnerability - Windows 7 SP1
287199717	2871997: Security Advisory: Update to fix the Pass-The-Hash Vulnerability - Windows 8 Gold
287641505	2876415: Windows RT, Windows 8, and Windows Server 2012 update rollup - KB2876415 - Windows 8 Gold (x64)
287641507	2876415: Windows RT, Windows 8, and Windows Server 2012 update rollup - KB2877211 - Windows 8 Gold (x64)
287641509	2876415: Windows RT, Windows 8, and Windows Server 2012 update rollup - KB2876415 - Windows 8 Gold
287641511	2876415: Windows RT, Windows 8, and Windows Server 2012 update rollup - KB2877211 - Windows 8 Gold
287721303	2877213: Applications disappear from the Start screen after you refresh a Windows RT, Windows 8, or Windows Server 2012-based computer by using a push-button reset recovery image - Windows 8 Gold
287721305	2877213: Applications disappear from the Start screen after you refresh a Windows RT, Windows 8, or Windows Server 2012-based computer by using a push-button reset recovery image - Windows 8 Gold (x64)
288278003	2882780: Incorrect UI color rendering when an application uses the D3D11CreateDevice or D3D10CreateDevice function in Windows - Windows 8 - KB2882780 (x64)

288278005	2882780: Incorrect UI color rendering when an application uses the D3D11CreateDevice or D3D10CreateDevice function in Windows - Windows 8 Gold
288320103	2883201: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold
288320105	2883201: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold (x64)
288753501	2887535: Update to Microsoft Update client - Windows 7 SP1
288804901	2888049: Update is available that improves the network performance of Internet Explorer 11 in Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows Server 2008 R2 SP1 (x64)
288804903	2888049: Update is available that improves the network performance of Internet Explorer 11 in Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 (x64)
288804905	2888049: Update is available that improves the network performance of Internet Explorer 11 in Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1
288954307	2889543: Text is corrupted when it's typed into a webpage that uses Adobe Flash Player after you install security update 2880289 - Windows 8 Gold
288954309	2889543: Text is corrupted when it's typed into a webpage that uses Adobe Flash Player after you install security update 2880289 - Windows 8 Gold (x64)
288978403	2889784: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold (x64)
288978405	2889784: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold
289057303	2890573: Update fixes coded UI test issues for Visual Studio 2010 SP1 in Internet Explorer 9 or Internet Explorer 10 when KB 2870699 is installed - Visual Studio 2010 SP1 - KB2890573
289121401	2891214: Update for the .NET Framework 4.5.1 and the .NET Framework 3.5 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 - Windows 8.1 Gold
289121403	2891214: Update for the .NET Framework 4.5.1 and the .NET Framework 3.5 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 - Windows 8.1 Gold / Windows Server 2012 R2 (x64)
289180405	2891804: Files or folders are removed unexpectedly when you perform a cut-and-paste operation on a Windows FTP client that is connected to an FTP site - Windows 7 SP1 (x64)
289180409	2891804: Files or folders are removed unexpectedly when you perform a cut-and-paste operation on a Windows FTP client that is connected to an FTP site - Windows 8 Gold (x64)

289180411	2891804: Files or folders are removed unexpectedly when you perform a cut-and-paste operation on a Windows FTP client that is connected to an FTP site - Windows 8 Gold
289180413	2891804: Files or folders are removed unexpectedly when you perform a cut-and-paste operation on a Windows FTP client that is connected to an FTP site - Windows 7 SP1
289363401	2893634: Performance of an application that calls the GetFileAttributesEx function degrades significantly in Windows 7 SP1 or Windows Server 2008 R2 SP1 - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)
289363403	2893634: Performance of an application that calls the GetFileAttributesEx function degrades significantly in Windows 7 SP1 or Windows Server 2008 R2 SP1 - Windows 7 SP1
289484211	2894842: Description of the security update for the .NET Framework 4 - .NET Framework 4.0 - Windows 7 SP1 / Windows 2003 SP2 / Windows 2008 SP2 / Windows Vista SP2 (x64) (V2.0)
289484213	2894842: Description of the security update for the .NET Framework 4 - .NET Framework 4.0 - Windows 7 SP1 / Windows 2003 SP2 / Windows 2008 SP2 / Windows Vista SP2 (V2.0)
289484311	2894843: Description of the security update for the .NET Framework 2.0 Service Pack 2 on Windows XP and Windows Server 2003 - Windows Server 2003 SP2 / Windows XP SP2 (x64)
289484313	2894843: Description of the security update for the .NET Framework 2.0 Service Pack 2 on Windows XP and Windows Server 2003 - Windows Server 2003 SP2 / Windows XP SP3
289484401	2894844: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1 - Windows 7 SP1 / Windows 2008 R2 SP1 (x64)
289484403	2894844: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1 - Windows 7 SP1
289484701	2894847: An update is available - .NET Framework 2.0 SP2 - Windows 2008 SP2 / Windows Vista SP2 (x64)
289484703	2894847: An update is available - .NET Framework 2.0 SP2 - Windows 2008 SP2 / Windows Vista SP2
289485101	2894851: Description of the security update for the .NET Framework 3.5 on Windows 8 and Windows Server 2012 - Windows 8 Gold / Windows Server 2012 Gold (x64)
289485103	2894851: Description of the security update for the .NET Framework 3.5 on Windows 8 and Windows Server 2012 - Windows 8 Gold
289485201	2894852: Description of the security update for the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 Gold / Windows Server 2012 R2 Gold (x64) (V2.0)

289485203	2894852: Description of the security update for the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 Gold (V2.0)
289485411	2894854: Description of the security update for the .NET Framework 4.5 and the .NET Framework 4.5.1 - .NET Framework 4.5/4.5.1 - Windows 7 SP1 / Windows 2008 SP2 / Windows 2008 R2 SP1 / Windows Vista SP2 (x64) (V2.0)
289485413	2894854: Description of the security update for the .NET Framework 4.5 and the .NET Framework 4.5.1 - .NET Framework 4.5/4.5.1 - Windows 7 SP1 / Windows 2008 SP2 / Windows Vista SP2 (V2.0)
289485503	2894855: Description of the security update for the .NET Framework 4.5 and the .NET Framework 4.5.1 on Windows 8, Windows RT, and Windows Server 2012 - .NET Framework 4.5/4.5.1 - Windows 8 Gold / Windows 2012 Gold (x64) (v2.0)
289485505	2894855: Description of the security update for the .NET Framework 4.5 and the .NET Framework 4.5.1 on Windows 8, Windows RT, and Windows Server 2012 - .NET Framework 4.5/4.5.1 - Windows 8 Gold (V2.0)
289485603	2894856: Description of the security update for the .NET Framework 4.5.1 on Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 - .NET Framework 4.5.1 - Windows 8.1 Gold / Windows 2012 R2 Gold (x64) (V2.0)
289485605	2894856: Description of the security update for the .NET Framework 4.5.1 on Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 - .NET Framework 4.5.1 - Windows 8.1 Gold (V2.0)
289568301	2895683: DNS record is deleted incorrectly after you disable DNS dynamic registration on a Windows client - Windows 7 SP1
289568303	2895683: DNS record is deleted incorrectly after you disable DNS dynamic registration on a Windows client - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)
289614601	2896146: Packet loss occurs when MTU is below 576 and PMTU discovery is enabled in Windows - Windows 8.1 Gold (x64)
289614605	2896146: Packet loss occurs when MTU is below 576 and PMTU discovery is enabled in Windows - Windows 8 Gold (x64)
289614609	2896146: Packet loss occurs when MTU is below 576 and PMTU discovery is enabled in Windows - Windows 7 SP1 (x64)
289614613	2896146: Packet loss occurs when MTU is below 576 and PMTU discovery is enabled in Windows - Windows 7 SP1
289614615	2896146: Packet loss occurs when MTU is below 576 and PMTU discovery is enabled in Windows - Windows 8 Gold
289614617	2896146: Packet loss occurs when MTU is below 576 and PMTU discovery is enabled in Windows - Windows 8.1 Gold
289884501	2898845: Description of the security update for the .NET Framework 3.5 on Windows 8 and Windows Server 2012 - Windows 8 Gold / 2012 Gold (x64)

289884503	2898845: Description of the security update for the .NET Framework 3.5 on Windows 8 and Windows Server 2012 - Windows 8 Gold
289884701	2898847: Description of the security update for the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 Gold / 2012 R2 Gold (x64)
289884703	2898847: Description of the security update for the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 Gold
289884903	2898849: Description of the security update for the .NET Framework 4.5, 4.5.1, and 4.5.2 - Windows 8 Gold / Windows 2012 Gold (x64)
289884905	2898849: Description of the security update for the .NET Framework 4.5, 4.5.1, and 4.5.2 - Windows 8 Gold
289885003	2898850: Description of the security update for the .NET Framework 4.5.1 and 4.5.2 - Windows 8.1 Gold / Windows 2012 R2 Gold (x64)
289885005	2898850: Description of the security update for the .NET Framework 4.5.1 and 4.5.2 - Windows 8.1 Gold
289885103	2898851: Description of the security update for the .NET Framework 3.5.1 - Windows 7 SP1 / Windows 2008 R2 SP1 (x64)
289885105	2898851: Description of the security update for the .NET Framework 3.5.1 - Windows 7 SP1
289918901	2899189: Update adds support for many camera-specific file formats in Windows 8.1 or Windows RT 8.1: December 2013 - Windows 8.1 Gold
289918905	2899189: Update adds support for many camera-specific file formats in Windows 8.1 or Windows RT 8.1: December 2013 - Windows 8.1 Gold (x64)
290154901	(2901549: Update improves the reliability of Internet Explorer 11 in Windows 8.1
290154903	2901549: Update improves the reliability of Internet Explorer 11 in Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 - Windows 8.1 Gold (x64)
290154905	2901549: Update improves the reliability of Internet Explorer 11 in Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 - Windows 8.1 Gold
290393801	2903938: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold (x64)
290393803	2903938: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold
290426609	2904266: December 2013 cumulative time zone update for Windows operating systems - Windows XP SP2 (x64)
290545403	2905454: An update is available that changes the currency symbol of Latvia to the euro in Windows - Windows 7 SP1 (x64)
290545411	2905454: An update is available that changes the currency symbol of Latvia to the euro in Windows - Windows 7 SP1

290545413	2905454: An update is available that changes the currency symbol of Latvia to the euro in Windows - Windows 8 Gold (x64)
290545415	2905454: An update is available that changes the currency symbol of Latvia to the euro in Windows - Windows 8 Gold
290878301	2908783: Data corruption occurs on iSCSI LUNs in Windows - Windows 7 SP1
290878307	2908783: Data corruption occurs on iSCSI LUNs in Windows - Windows 7 SP1 (x64)
291110101	2911101: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold (x64)
291110105	2911101: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold
291315201	2913152: Windows Photo Viewer prints white lines when you use an XPS driver to print photos in Windows - Windows 8 Gold (x64)
291315215	2913152: Windows Photo Viewer prints white lines when you use an XPS driver to print photos in Windows - Windows 8 Gold
291323601	2913236: You may experience poor battery life on a Lenovo Miix2 8 tablet running Windows 8.1 - Windows 8.1 Gold
291448603	2914486: Microsoft Security Advisory - Vulnerability in Microsoft Windows Kernel Could Allow Elevation of Privilege - Disable Workaround - Windows XP SP3 / Windows Server 2003 SP2
291748801	2917488: Dynamic Update for Windows 8.1 - Windows 8.1 Gold
291748803	2917488: Dynamic Update for Windows 8.1 - Windows 8.1 Gold (x64)
291807701	2918077: VAN UI freezes after KB2813956 is applied in Windows 7 - Windows 7 SP1 (x64)
291807703	2918077: VAN UI freezes after KB2813956 is applied in Windows 7 - Windows 7 SP1
291935501	2919355: Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 Update - KB2919355 - Windows 8.1 Gold (x64)
291935513	2919355: Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 Update - KB2919355 - Windows 8.1 Gold
291939301	2919393: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold (x64)
291939305	2919393: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold
291944203	2919442: A servicing stack update is available - Windows 8.1 Gold (x64)
291944205	2919442: A servicing stack update is available - Windows 8.1 Gold
292191601	2921916: The "Untrusted publisher" dialog box appears when you install a driver in Windows 7 or Windows Server 2008 R2 - Windows 7 SP1
292191605	2921916: The "Untrusted publisher" dialog box appears when you install a driver in Windows 7 or Windows Server 2008 R2 - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)

292222301	2922223: You cannot change system time if RealTimeIsUniversal registry entry is enabled in Windows - Windows 7 SP1 - KB2922223 (x64)
292222307	2922223: You cannot change system time if RealTimeIsUniversal registry entry is enabled in Windows - Windows 7 SP1 - KB2922223
292354503	2923545: Update for RDP 8.1 is available for Windows 7 SP1 - Windows 7 SP1 (x64)
292354505	2923545: Update for RDP 8.1 is available for Windows 7 SP1 - Windows 7 SP1
292867803	2928678: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold (x64)
292867805	2928678: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold
292973307	2929733: The first stage of the WER protocol is not SSL encrypted in Windows - Windows Vista SP2
292973313	2929733: The first stage of the WER protocol is not SSL encrypted in Windows - Windows Vista SP2 (x64)
292987403	2929874: "The parameter is incorrect" error when you run Defrag.Exe in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 - KB2929874
293235401	2932354: Update for Embedded Lockdown Manager on Windows Embedded 8 Standard and Windows Embedded 8.1 Industry devices - Windows 7 SP1 - KB2932354 (x64)
293235403	2932354: Update for Embedded Lockdown Manager on Windows Embedded 8 Standard and Windows Embedded 8.1 Industry devices - Windows 7 SP1 - KB2932354
293401601	2934016: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold
293401603	2934016: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold (x64)
293509207	2935092: Daylight saving time (DST) changes for Chile, Turkey, and Paraguay - Windows 7 SP1
293509209	2935092: Daylight saving time (DST) changes for Chile, Turkey, and Paraguay - Windows Vista SP2
293509213	2935092: Daylight saving time (DST) changes for Chile, Turkey, and Paraguay - Windows 8 Gold (x64)
293509219	2935092: Daylight saving time (DST) changes for Chile, Turkey, and Paraguay - Windows 8.1 Gold (x64)
293509225	(2935092: Daylight saving time (DST) changes for Chile
293509227	2935092: Daylight saving time (DST) changes for Chile, Turkey, and Paraguay - Windows 8 Gold
293509233	2935092: Daylight saving time (DST) changes for Chile, Turkey, and Paraguay - Windows 8.1 Gold
293509237	2935092: Daylight saving time (DST) changes for Chile, Turkey, and Paraguay - Windows Vista SP2 (x64)

293509239	2935092: Daylight saving time (DST) changes for Chile, Turkey, and Paraguay - Windows 7 SP1 (x64)
293845901	2938459: Windows Communications Apps update for Windows 8 and Windows RT - Windows 8 Gold
293845903	2938459: Windows Communications Apps update for Windows 8 and Windows RT - Windows 8 Gold (x64)
293878003	2938780: Description of the security update for the .NET Framework 4 - Windows 7 SP1 / Windows 2008 R2 SP1 (x64)
293878005	2938780: Description of the security update for the .NET Framework 4 - Windows 7 SP1 / Windows 2003 SP2 / Windows 2008 SP2 / Windows Vista SP2
293878201	2938782: Description of the security update for the .NET Framework 4.5 and 4.5.1 - Windows 7 SP1 / Windows 2008 R2 SP1 (x64)
293878203	2938782: Description of the security update for the .NET Framework 4.5 and 4.5.1 - Windows 7 SP1
295485303	2954853: Description of the security update for the .NET Framework 4.5.2 - Windows 7 SP1
295487903	2954879: Description of the update for .NET Native in Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 - Windows 8.1 Gold / Windows Server 2012 R2 Gold (x64)
295487905	2954879: Description of the update for .NET Native in Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 - Windows 8.1 Gold
295516303	2955163: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold (x64)
295516305	2955163: Windows RT, Windows 8, and Windows Server 2012 update rollup - Windows 8 Gold
295580801	2955808: A VPN connection through a third-party VPN server disconnects after an hour on a Windows-based computer - Windows 8 Gold (x64)
295580803	2955808: A VPN connection through a third-party VPN server disconnects after an hour on a Windows-based computer - Windows 8 Gold
295962601	2959626: Reliability improvements for Remote Desktop Session Host and RemoteApp - Windows 8.1 Gold (x64)
295962605	2959626: Reliability improvements for Remote Desktop Session Host and RemoteApp - Windows 8.1 Gold
296083701	2960837: Excel freezes when you convert Japanese characters in Windows - Windows 8 Gold (x64)
296083705	2960837: Excel freezes when you convert Japanese characters in Windows - Windows 8 Gold
296215601	2962156: Camera app update for WSUS for Windows 8 - Windows 8 Gold
296215603	2962156: Camera app update for WSUS for Windows 8 - Windows 8 Gold (x64)

296216301	2962163: Xbox Video app update for WSUS for Windows 8 - Windows 8 Gold
296216303	2962163: Xbox Video app update for WSUS for Windows 8 - Windows 8 Gold (x64)
296216801	2962168: Photos app update for WSUS for Windows 8 - Windows 8 Gold
296216803	2962168: Photos app update for WSUS for Windows 8 - Windows 8 Gold
296216901	2962169: Xbox Games app update for WSUS for Windows 8 - Windows 8 Gold
296216903	2962169: Xbox Games app update for WSUS for Windows 8 - Windows 8 Gold (x64)
296217101	2962171: Xbox Music app update for WSUS for Windows 8 - Windows 8 Gold
296217103	2962171: Xbox Music app update for WSUS for Windows 8 - Windows 8 Gold (x64)
296217301	2962173: Bing Finance app update for WSUS for Windows 8 - Windows 8 Gold
296217303	2962173: Bing Finance app update for WSUS for Windows 8 - Windows 8 Gold (x64)
296217501	2962175: Bing News app update for WSUS for Windows 8 - Windows 8 Gold
296217503	2962175: Bing News app update for WSUS for Windows 8 - Windows 8 Gold (x64)
296217601	2962176: Bing Sports app update for WSUS for Windows 8 - Windows 8 Gold
296217603	2962176: Bing Sports app update for WSUS for Windows 8 - Windows 8 Gold
296217701	2962177: Bing Travel app update for WSUS for Windows 8 - Windows 8 Gold
296217703	2962177: Bing Travel app update for WSUS for Windows 8 - Windows 8 Gold (x64)
296217801	2962178: Bing Weather app update for WSUS for Windows 8 - Windows 8 Gold
296217803	2962178: Bing Weather app update for WSUS for Windows 8 - Windows 8 Gold (x64)
296217901	2962179: Bing Search app update for WSUS for Windows 8 - Windows 8 Gold
296217903	2962179: Bing Search app update for WSUS for Windows 8 - Windows 8 Gold (x64)
296218001	2962180: Bing Maps app update for WSUS for Windows 8 - Windows 8 Gold
296218003	2962180: Bing Maps app update for WSUS for Windows 8 - Windows 8 Gold (x64)
296218101	2962181: Reader app update for WSUS for Windows 8 - Windows 8 Gold

296218103	2962181: Reader app update for WSUS for Windows 8 - Windows 8 Gold (x64)
296218301	2962183: Xbox Games app update for WSUS for Windows 8.1 - Windows 8.1 Gold
296218303	2962183: Xbox Games app update for WSUS for Windows 8.1 - Windows 8.1 Gold (x64)
296218401	2962184: Xbox Music app update for WSUS for Windows 8.1 - Windows 8.1 Gold
296218403	2962184: Xbox Music app update for WSUS for Windows 8.1 - Windows 8.1 Gold
296218501	2962185: Xbox Video app update for WSUS for Windows 8.1 - Windows 8.1 Gold
296218503	2962185: Xbox Video app update for WSUS for Windows 8.1 - Windows 8.1 Gold
296219301	2962193: Reader app update for WSUS for Windows 8.1 - Windows 8.1 Gold
296219303	2962193: Reader app update for WSUS for Windows 8.1 - Windows 8.1 Gold (x64)
296219401	2962194: Help and Tips app update for WSUS for Windows 8.1 - Windows 8.1 Gold
296219403	2962194: Help and Tips app update for WSUS for Windows 8.1 - Windows 8.1 Gold (x64)
296219501	2962195: Windows Reading List app update for WSUS for Windows 8.1 - Windows 8.1 Gold
296219503	2962195: Windows Reading List app update for WSUS for Windows 8.1 - Windows 8.1 Gold (x64)
296219601	2962196: Calculator app update for WSUS for Windows 8.1 - Windows 8.1 Gold
296219603	2962196: Calculator app update for WSUS for Windows 8.1 - Windows 8.1 Gold (x64)
296219701	2962197: Alarms app update for WSUS for Windows 8.1 - Windows 8.1 Gold
296219703	2962197: Alarms app update for WSUS for Windows 8.1 - Windows 8.1 Gold (x64)
296219801	2962198: Sound Recorder app update for WSUS for Windows 8.1 - Windows 8.1 Gold
296219803	2962198: Sound Recorder app update for WSUS for Windows 8.1 - Windows 8.1 Gold (x64)
296219901	2962199: Bing Food & Drink app update for WSUS for Windows 8.1 - Windows 8.1 Gold
296219903	2962199: Bing Food & Drink app update for WSUS for Windows 8.1 - Windows 8.1 Gold (x64)

296220001	2962200: Scan app update for WSUS for Windows 8.1 - Windows 8.1 Gold
296220003	2962200: Scan app update for WSUS for Windows 8.1 - Windows 8.1 Gold (x64)
296220101	2962201: Skype app update for WSUS for Windows 8.1 - Windows 8.1 Gold
296220103	2962201: Skype app update for WSUS for Windows 8.1 - Windows 8.1 Gold (x64)
296239301	2962393: Security Advisory: Update for vulnerability in Juniper Networks Windows In-Box Junos Pulse client (KB2964757) - Windows 8.1 Gold
296239303	2962393: Security Advisory: Update for vulnerability in Juniper Networks Windows In-Box Junos Pulse client (KB2964757) - Windows 8.1 Gold (x64)
296240701	2962407: Windows RT, Windows 8, and Windows Server 2012 update rollup - KB2962407 - Windows 8 Gold (x64)
296240703	2962407: Windows RT, Windows 8, and Windows Server 2012 update rollup - KB2962407 - Windows 8 Gold
296282403	2962824: Security Advisory: Update rollup of revoked noncompliant UEFI modules - Windows 8 Gold (x64)
296282405	2962824: Security Advisory: Update rollup of revoked noncompliant UEFI modules - Windows 8 Gold
296398303	2963983: Vulnerability in Internet Explorer Could Allow Remote Code Execution - Disable Workaround (x64)
296398307	2963983: Vulnerability in Internet Explorer Could Allow Remote Code Execution - Disable Workaround
296535105	2965351: "Error_FILE_NOT_FOUND" when you print to a shared network printer - Windows 8 Gold
296535109	2965351: "Error_FILE_NOT_FOUND" when you print to a shared network printer - Windows 8 Gold / Windows Server 2012 Gold (x64)
296791601	2967916: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB2967916 - Windows 8 Gold (x64)
296791605	2967916: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB2967916 - Windows 8 Gold
296791703	2967917: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - KB2967917 - Windows 8.1 Gold (x64)
296791705	2967917: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - KB2967917 - Windows 8.1 Gold
297022805	2970228: Update to support the new currency symbol for the Russian ruble in Windows - KB2970228 - Windows 7 SP1 (x64)
297022809	2970228: Update to support the new currency symbol for the Russian ruble in Windows - KB2970228 - Windows 7 SP1

297335101	2973351: Security Advisory: Registry update to improve credentials protection and management for Windows-based systems that have the 2919355 update installed - Windows 8 Gold
297335109	2973351: Security Advisory: Registry update to improve credentials protection and management for Windows-based systems that have the 2919355 update installed - Windows 7 SP1
297335115	2973351: Security Advisory: Registry update to improve credentials protection and management for Windows-based systems that have the 2919355 update installed - Windows 8 Gold (x64)
297335121	2973351: Security Advisory: Registry update to improve credentials protection and management for Windows-based systems that have the 2919355 update installed - Windows 7 SP1 (x64)
297350103	2973501: Update to support RDP restricted administration for Windows 8 and Windows Server 2012 - Windows 8 Gold
297350105	2973501: Update to support RDP restricted administration for Windows 8 and Windows Server 2012 - Windows 8 Gold (x64)
297533105	2975331: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB2975331 - Windows 8 Gold (x64)
297533107	2975331: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB2993651 - Windows 8 Gold (x64)
297533109	2975331: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB2975331 - Windows 8 Gold
297533111	2975331: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB2993651 - Windows 8 Gold
297571915	2975719: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - KB2979582 - Windows 8.1 Gold
297571917	2975719: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - KB2990532 - Windows 8.1 Gold
297571919	2975719: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - KB2993100 - Windows 8.1 Gold
297571923	2975719: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - KB2995004 - Windows 8.1 Gold
297571927	2975719: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - KB2979582 - Windows 8.1 Gold (x64)
297571929	2975719: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - KB2990532 - Windows 8.1 Gold (x64)
297571931	2975719: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - KB2993100 - Windows 8.1 Gold (x64)
297571935	2975719: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - KB2995004 - Windows 8.1 Gold (x64)
297697801	2976978: Compatibility update for keeping Windows up-to-date in Windows 8.1 and Windows 8 - Windows 8.1 - KB2976978 (V23.0)

297697803	2976978: Compatibility update for Windows 8.1 and Windows 8 - Windows 8 - KB2976978 (V16.0)
297697805	2976978: Compatibility update for keeping Windows up-to-date in Windows 8.1 and Windows 8 - Windows 8.1 - KB2976978 (x64) (V23.0)
297697807	2976978: Compatibility update for Windows 8.1 and Windows 8 - Windows 8 - KB2976978 (x64) (V16.0)
297729209	2977292: Security advisory: Update for Microsoft EAP implementation that enables the use of TLS - Windows 7 SP1
297729211	2977292: Security advisory: Update for Microsoft EAP implementation that enables the use of TLS - Windows 7 SP1 (x64)
297729217	2977292: Security advisory: Update for Microsoft EAP implementation that enables the use of TLS - Windows 8 Gold
297729221	2977292: Security advisory: Update for Microsoft EAP implementation that enables the use of TLS - Windows 8 Gold (x64)
297775901	2977759: Compatibility update for Windows 7 RTM - Windows 7 SP1 - KB2977759 (V15.0)
297775903	2977759: Compatibility update for Windows 7 RTM - Windows 7 SP1 - KB2977759 (x64) (V15.0)
297775905	2977759: Compatibility update for Windows 7 RTM - Windows 7 Gold - KB2977759 (x64) (V12.0)
297775907	2977759: Compatibility update for Windows 7 RTM - Windows 7 Gold - KB2977759 (V12.0)
298065401	2980654: OneDrive reliability update for Windows 8.1 and Windows RT 8.1 - Windows 8.1 Gold (x64)
298065403	2980654: OneDrive reliability update for Windows 8.1 and Windows RT 8.1 - Windows 8.1 Gold
298400501	2984005: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB2977174 - Windows 8 Gold
298400503	2984005: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB2984005 - Windows 8 Gold
298400505	2984005: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB2977174 - Windows 8 Gold (x64)
298400507	2984005: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB2984005 - Windows 8 Gold (x64)
298497203	2984972: Update for RDC 7.1 to support restricted administration logons on Windows 7 and Windows Server 2008 R2 - Windows 7 SP1 (x64)
298497211	2984972: Update for RDC 7.1 to support restricted administration logons on Windows 7 and Windows Server 2008 R2 - Windows 7 SP1
298497603	2984976: RDP 8.0 update for restricted administration on Windows 7 or Windows Server 2008 R2 - Windows 7 SP1
298497605	2984976: RDP 8.0 update for restricted administration on Windows 7 or Windows Server 2008 R2 - Windows 7 SP1 (x64)

298546103	2985461: Error 0x800401f0 when you update RemoteApp and Desktop Connections feeds in Windows 7 or Windows Server 2008 R2 - Windows 7 SP1
298546105	2985461: Error 0x800401f0 when you update RemoteApp and Desktop Connections feeds in Windows 7 or Windows Server 2008 R2 - Windows 7 SP1 (x64)
298993001	2989930: "Not Connected" status for a paired Surface Pen in Bluetooth settings on Surface Pro 3 - Windows 8.1 Gold (x64)
298993005	2989930: "Not Connected" status for a paired Surface Pen in Bluetooth settings on Surface Pro 3 - Windows 8.1 Gold
299094101	2990941: Update to add native driver support in NVM Express in Windows 7 and Windows Server 2008 R2 - Windows 7 SP1 - KB2990941
299094103	2990941: Update to add native driver support in NVM Express in Windows 7 and Windows Server 2008 R2 - Windows 7 SP1 / Windows Server 2008 R2 SP1 - KB2990941 (x64)
299096701	2990967: Some versions of the OneDrive desktop app for Windows do not update automatically - Windows 8.1 Gold (x64)
299096703	2990967: Some versions of the OneDrive desktop app for Windows do not update automatically - Windows 8.1 Gold
299429001	2994290: Language Interface Pack for Windows 8.1 and Windows RT 8.1 - Windows 8.1 Gold
299429003	2994290: Language Interface Pack for Windows 8.1 and Windows RT 8.1 - Windows 8.1 Gold (x64)
299505401	2995054: SMBv1 named pipe requests do not time out when the remote server hangs in Windows 7, Windows Server 2008, Windows 8.1, and Windows Server 2012 R2 - Windows 8.1 Gold (x64) / Windows Server 2012 R2 (x64)
299505407	2995054: SMBv1 named pipe requests do not time out when the remote server hangs in Windows 7, Windows Server 2008, Windows 8.1, and Windows Server 2012 R2 - Windows 8.1 Gold
299538701	2995387: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - Windows 8 Gold (x64)
299538703	2995387: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - Windows 8 Gold
299881201	2998812: Compatibility update for Windows 7 or Windows Server 2008 R2 - Windows 7 Gold
299881203	2998812: Compatibility update for Windows 7 or Windows Server 2008 R2 - Windows 7 Gold / Windows Server 2008 R2 Gold (x64)
299922609	2999226: Update for Universal C Runtime in Windows - Windows Vista SP2 (x64)
299922613	2999226: Update for Universal C RunTime in Windows - Windows 8 Gold (x64)

299922617	2999226: Update for Universal C Runtime in Windows - Windows Vista SP2
299922619	2999226: Update for Universal C RunTime in Windows - Windows 8 Gold
300085001	3000850: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - KB3000850 - Windows 8.1 Gold (x64)
300085003	3000850: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - KB3003057 - Windows 8.1 Gold (x64)
300085005	3000850: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - KB3014442 - Windows 8.1 Gold (x64)
300085015	3000850: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - KB3000850 - Windows 8.1 Gold
300085017	3000850: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - KB3003057 - Windows 8.1 Gold
300085019	3000850: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - KB3014442 - Windows 8.1 Gold
300085301	3000853: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB3000853 - Windows 8 Gold
300085303	3000853: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB3000853 - Windows 8 Gold (x64)
300085307	3000853: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB2996928 - Windows 8 Gold (x64)
300085311	3000853: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB2996928 - Windows 8 Gold
300285901	3002859: Miracast display resolution changes after you shut down and then restart a Windows 8.1-based computer - Windows 8.1 Gold (x64) / Windows Server 2012 R2 Gold (x64)
300285903	3002859: Miracast display resolution changes after you shut down and then restart a Windows 8.1-based computer - Windows 8.1 Gold
300366301	3003663: Update to support many camera-specific file formats in Windows 8 and Windows RT - Windows 8 Gold (x64)
300366303	3003663: Update to support many camera-specific file formats in Windows 8 and Windows RT - Windows 8 Gold
300366701	3003667: Update to support many camera-specific file formats in Windows 8.1 and Windows RT 8.1 - Windows 8.1 Gold (x64)
300366703	3003667: Update to support many camera-specific file formats in Windows 8.1 and Windows RT 8.1 - Windows 8.1 Gold
300372701	3003727: USB 3.0 debugger through a USB 2.0 port is not supported on Intel System-on-Chip (SoC) devices in Windows 8.1 - Windows 8.1 Gold
300372703	3003727: USB 3.0 debugger through a USB 2.0 port is not supported on Intel System-on-Chip (SoC) devices in Windows 8.1 - Windows 8.1 Gold (x64) / Windows Server 2012 R2 (x64)

300372705	3003727: USB 3.0 debugger through a USB 2.0 port is not supported on Intel System-on-Chip (SoC) devices in Windows 8.1 - KB3008242 - Windows 8.1 Gold
300372707	3003727: USB 3.0 debugger through a USB 2.0 port is not supported on Intel System-on-Chip (SoC) devices in Windows 8.1 - KB3008242 - Windows 8.1 Gold (x64) / Windows Server 2012 R2 (x64)
300437503	3004375: Security advisory: Update to improve Windows command-line auditing - Windows 7 SP1 (x64)
300437507	3004375: Security advisory: Update to improve Windows command-line auditing - Windows 7 SP1
300437509	3004375: Security advisory: Update to improve Windows command-line auditing - Windows 8 Gold
300437515	3004375: Security advisory: Update to improve Windows command-line auditing - Windows 8 Gold (x64)
300439405	3004394: Support for urgent Trusted Root updates for Windows Root Certificate Program in Windows - Windows 8 Gold (x64)
300439407	3004394: Support for urgent Trusted Root updates for Windows Root Certificate Program in Windows - Windows 8 Gold
300454501	3004545: You cannot access virtual machines that are hosted on Azure hosting services through a VPN connection in Windows - Windows 8.1 Gold / Windows Server 2012 R2 Gold (x64)
300454503	3004545: You cannot access virtual machines that are hosted on Azure hosting services through a VPN connection in Windows - Windows 8.1 Gold
300562801	3005628: Update for the .NET Framework 3.5 on Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2 - Windows 8 Gold
300562803	3005628: Update for the .NET Framework 3.5 on Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2 - Windows 8.1 Gold
300562805	3005628: Update for the .NET Framework 3.5 on Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2 - Windows 8 Gold / Windows Server 2012 Gold (x64)
300562807	3005628: Update for the .NET Framework 3.5 on Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2 - Windows 8.1 Gold / Windows Server 2012 R2 Gold (x64)
300612103	3006121: Private EDUCs are not displayed in Character Map after you apply update 2982791 in Windows 7 or Windows Server 2008 R2 - Windows 7 SP1 (x64)
300612105	3006121: Private EDUCs are not displayed in Character Map after you apply update 2982791 in Windows 7 or Windows Server 2008 R2 - Windows 7 SP1
300613703	3006137: Update changes the currency symbol of Lithuania from the Lithuanian litas (Lt) to the euro in Windows - Windows 8 Gold

300613705	3006137: Update changes the currency symbol of Lithuania from the Lithuanian litas (Lt) to the euro in Windows - Windows 7 SP1
300613707	3006137: Update changes the currency symbol of Lithuania from the Lithuanian litas (Lt) to the euro in Windows - Windows 8 Gold (x64)
300613719	3006137: Update changes the currency symbol of Lithuania from the Lithuanian litas (Lt) to the euro in Windows - Windows 7 SP1 (x64)
300827301	3008273: An update to enable an automatic update from Windows 8 to Windows 8.1 - Windows 8 Gold (x64) (v4.0)
300827303	3008273: An update to enable an automatic update from Windows 8 to Windows 8.1 - Windows 8 Gold (v4.0)
300900805	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for IE Settings (Disable SSL 3.0 and enable TLS 1.0, TLS 1.1, and TLS 1.2 in Internet Explorer)
300900807	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Enable Workaround for Server Software (Disable SSL 3.0 in Windows)
300900809	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for Server Software (Disable SSL 3.0 in Windows)
300900811	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Enable Workaround for Client Software (Disable SSL 3.0 in Windows)
300900813	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for Client Software (Disable SSL 3.0 in Windows)
300900817	3009008: Security Advisory: Vulnerability in SSL 3.0 Could Allow Information Disclosure - Disable Workaround for IE Settings (Disable SSL 3.0 in Internet Explorer)
301223503	3012235: The Print Pictures Wizard stops responding in Windows 8.1 - Windows 8.1 Gold (x64)
301223505	3012235: The Print Pictures Wizard stops responding in Windows 8.1 - Windows 8.1 Gold
301270205	3012702: Some default program associations for a roamed user may be lost when you log on to an RDS server in Windows - Windows 8 Gold (x64)
301270207	3012702: Some default program associations for a roamed user may be lost when you log on to an RDS server in Windows - Windows 8 Gold
301270209	3012702: Some default program associations for a roamed user may be lost when you log on to an RDS server in Windows - Windows 8.1 Gold (x64)
301270211	3012702: Some default program associations for a roamed user may be lost when you log on to an RDS server in Windows - Windows 8.1 Gold
301317201	3013172: Individual memory devices cannot be ejected through the Safely Remove Hardware UI in Windows 8.1 - Windows 8.1 Gold (x64)

301317205	3013172: Individual memory devices cannot be ejected through the Safely Remove Hardware UI in Windows 8.1 - Windows 8.1 Gold
301353101	3013531: Update to support copying .mkv files to Windows Phone from a computer that is running Windows - Windows 7 SP1
301353103	3013531: Update to support copying .mkv files to Windows Phone from a computer that is running Windows - Windows 8 Gold (x64)
301353105	3013531: Update to support copying .mkv files to Windows Phone from a computer that is running Windows - Windows 7 SP1 (x64)
301353107	3013531: Update to support copying .mkv files to Windows Phone from a computer that is running Windows - Windows 8.1 Gold (x64)
301353109	3013531: Update to support copying .mkv files to Windows Phone from a computer that is running Windows - Windows 8 Gold
301353111	3013531: Update to support copying .mkv files to Windows Phone from a computer that is running Windows - Windows 8.1 Gold
301353801	3013538: Automatic brightness option is disabled unexpectedly after you switch between PC settings pages in Windows - Windows 8.1 Gold (x64)
301353805	3013538: Automatic brightness option is disabled unexpectedly after you switch between PC settings pages in Windows - Windows 8.1 Gold
301376701	3013767: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB2999323 - Windows 8 Gold (x64)
301376703	3013767: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB3013767 - Windows 8 Gold (x64)
301376705	3013767: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB2999323 - Windows 8 Gold
301376707	3013767: Update rollup for Windows RT, Windows 8, and Windows Server 2012 - KB3013767 - Windows 8 Gold
301376901	3013769: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - Windows 8.1 Gold (x64)
301376905	3013769: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - Windows 8.1 Gold
301379101	3013791: "DPC_WATCHDOG_VIOLATION (0x133)" Stop error when there's faulty hardware in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 Gold (x64)
301379105	3013791: "DPC_WATCHDOG_VIOLATION (0x133)" Stop error when there's faulty hardware in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 Gold
301381603	3013816: MDM client update in Windows - Windows 8.1 Gold (x64)
301381605	3013816: MDM client update in Windows - Windows 8.1 Gold
301569601	3015696: The InputPersonalization.exe process crashes in Windows - Windows 8.1 Gold
301569603	3015696: The InputPersonalization.exe process crashes in Windows - Windows 8.1 Gold (x64)

301813301	3018133: Content on the lock screen is displayed inappropriately in Windows that has update 2919355 installed - Windows 8.1 Gold
301813305	3018133: Content on the lock screen is displayed inappropriately in Windows that has update 2919355 installed - Windows 8.1 Gold (x64)
302033801	3020338: Line of business applications cannot start after you apply update 3006226 in Windows - Windows 8 Gold (x64)
302033833	3020338: Line of business applications cannot start after you apply update 3006226 in Windows - Windows 8 Gold
302037001	3020370: Update the copy of the Cmitrust.dll file in Windows - Windows 7 SP1
302037003	3020370: Update the copy of the Cmitrust.dll file in Windows - Windows 8 Gold
302037005	3020370: Update the copy of the Cmitrust.dll file in Windows - Windows 8 Gold (x64)
302037011	3020370: Update the copy of the Cmitrust.dll file in Windows - Windows 8.1 Gold
302037013	3020370: Update the copy of the Cmitrust.dll file in Windows - Windows 8.1 Gold (x64)
302037015	3020370: Update the copy of the Cmitrust.dll file in Windows - Windows 7 SP1 (x64)
302191701	3021917: Update to Windows 7 SP1 for performance improvements - Windows 7 SP1 (x64)
302191703	3021917: Update to Windows 7 SP1 for performance improvements - Windows 7 SP1
302475101	3024751: The TAB key inserts a tab stop when you enter Wi-Fi credentials on a Surface Pro 3 - Windows 8.1 Gold (x64)
302475103	3024751: The TAB key inserts a tab stop when you enter Wi-Fi credentials on a Surface Pro 3 - Windows 8.1 Gold
302475503	3024755: Multi-touch gesture does not work after you exit the Calculator in Windows - Windows 8.1 Gold (x64)
302475505	3024755: Multi-touch gesture does not work after you exit the Calculator in Windows - Windows 8.1 Gold
302477701	3024777: Install KB3024777 to fix an issue with KB3004394 on Windows 7 and Windows Server 2008 R2 - Windows 7 Gold
302594501	3025945: Internet Explorer 9 stops working after you install update 3008923 in Windows - Windows Server 2008 SP2
302594503	3025945: Internet Explorer 9 stops working after you install update 3008923 in Windows - Windows 7 SP1
302594505	3025945: Internet Explorer 9 stops working after you install update 3008923 in Windows - Windows Server 2008 SP2 (x64)
302594507	3025945: Internet Explorer 9 stops working after you install update 3008923 in Windows - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64)

302720901	3027209: Reliability improvements for Windows 8.1: March 2015 - Windows 8.1 Gold (x64)
302720905	3027209: Reliability improvements for Windows 8.1: March 2015 - Windows 8.1 Gold
302960301	3029603: xHCI driver crashes after you resume computer from sleep mode in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 Gold (x64)
302960303	3029603: xHCI driver crashes after you resume computer from sleep mode in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 Gold
302960601	3029606: Update to improve Bluetooth driver diagnosis in Windows 8.1 - Windows 8.1 Gold (V2.0)
302960603	3029606: Update to improve Bluetooth driver diagnosis in Windows 8.1 - Windows 8.1 Gold (x64) (V2.0)
303094701	3030947: Compatibility issues for applications that rely on a certain code layout for memory in Windows - Windows 8.1 Gold (x64)
303094703	3030947: Compatibility issues for applications that rely on a certain code layout for memory in Windows - Windows 8.1 Gold
303104401	3031044: The Embedded Lockdown Manager application is installed unexpectedly in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 Gold
303104403	3031044: The Embedded Lockdown Manager application is installed unexpectedly in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 Gold / Windows Server 2012 R2 Gold (x64)
303261301	3032613: Text in Polish, Bulgarian, or Greek does not display completely on the Windows Store installation page in Windows - Windows 8 Gold (x64)
303261303	3032613: Text in Polish, Bulgarian, or Greek does not display completely on the Windows Store installation page in Windows - Windows 8 Gold
303344603	3033446: Wi-Fi connectivity issues or poor performance on CHT platform computers in Windows 8.1 - Windows 8.1 Gold (x64)
303344605	3033446: Wi-Fi connectivity issues or poor performance on CHT platform computers in Windows 8.1 - Windows 8.1 Gold
303552701	3035527: Problems occur after you pin and unpin a Win32 app from the taskbar in Windows - Windows 8.1 Gold (x64)
303552705	3035527: Problems occur after you pin and unpin a Win32 app from the taskbar in Windows - Windows 8.1 Gold
303620001	3036200: Update for Embedded Lockdown Manager on Windows Embedded 8 Standard and Windows Embedded 8.1 Industry devices - Windows 8 - KB3036200 (x64)
303620023	3036200: Update for Embedded Lockdown Manager on Windows Embedded 8 Standard and Windows Embedded 8.1 Industry devices - Windows 8 - KB3036200

303661201	3036612: Windows Store apps may crash in Windows 8.1 or Windows RT 8.1 - Windows 8.1 Gold
303661205	3036612: Windows Store apps may crash in Windows 8.1 or Windows RT 8.1 - Windows 8.1 Gold (x64)
303763907	3037639: Fix for text quality degradation after security update 3013455 (MS15-010) is installed - Windows Vista SP2
303763915	3037639: Fix for text quality degradation after security update 3013455 (MS15-010) is installed - Windows Vista SP2 (x64)
303792401	3037924: You cannot do System Image Backup to Blu-ray media in Windows - Windows 8.1 Gold
303792405	3037924: You cannot do System Image Backup to Blu-ray media in Windows - Windows 8.1 Gold (x64)
303800203	3038002: UHS-3 cards cannot be detected in Windows on Surface devices - Windows 8.1 Gold (x64)
303800205	3038002: UHS-3 cards cannot be detected in Windows on Surface devices - Windows 8.1 Gold
303825611	3038256: Update for Embedded Lockdown Manager on Windows Embedded 8 Standard and Windows Embedded 8.1 Industry devices - Windows 8.1 - KB3038256 (x64)
303825623	3038256: Update for Embedded Lockdown Manager on Windows Embedded 8 Standard and Windows Embedded 8.1 Industry devices - Windows 8.1 - KB3038256
303893601	3038936: Anti-malware platform update for Windows Defender in Windows 8.1 and Windows 8 - Windows 8 Gold (x64)
303893605	3038936: Anti-malware platform update for Windows Defender in Windows 8.1 and Windows 8 - Windows 8 Gold
303902403	3039024: Daylight saving time changes for Chile and Mexico in Windows - Windows Vista SP2 / Windows Server 2008 SP2 (x64)
304027201	3040272: Start time increases after another language pack is added to Windows - Windows 8 Gold (x64)
304027203	3040272: Start time increases after another language pack is added to Windows - Windows 8 Gold
304205805	3042058: Security advisory: Update to default cipher suite priority order - Windows 7 SP1 - KB3042058
304205811	3042058: Security advisory: Update to default cipher suite priority order - Windows 7 SP1 - KB3042058 (x64)
304205813	3042058: Security advisory: Update to default cipher suite priority order - Windows 8.1 - KB3042058 (x64)
304205817	3042058: Security advisory: Update to default cipher suite priority order - Windows 8.1 - KB3042058
304205819	3042058: Security advisory: Update to default cipher suite priority order - Windows 8 - KB3042058

304205823	3042058: Security advisory: Update to default cipher suite priority order - Windows 8 - KB3042058 (x64)
304208501	3042085: Device does not respond during shutdown after you have installed November 2014 update in Windows - Windows 8.1 Gold (x64)
304208503	3042085: Device does not respond during shutdown after you have installed November 2014 update in Windows - Windows 8.1 Gold
304381203	3043812: Layout of Cambria font is different in Word documents when the text metric changes in Windows 8.1 or Windows 8 - Windows 8 Gold
304381205	3043812: Layout of Cambria font is different in Word documents when the text metric changes in Windows 8.1 or Windows 8 - Windows 8.1 Gold
304381209	3043812: Layout of Cambria font is different in Word documents when the text metric changes in Windows 8.1 or Windows 8 - Windows 8 Gold (x64)
304381211	3043812: Layout of Cambria font is different in Word documents when the text metric changes in Windows 8.1 or Windows 8 - Windows 8.1 Gold (x64)
304437403	3044374: Update that enables you to upgrade from Windows 8.1 to a later version of Windows - Windows 8.1 Gold (x64)
304437405	3044374: Update that enables you to upgrade from Windows 8.1 to a later version of Windows - Windows 8.1 Gold
304467301	3044673: Photos taken by certain Android devices show blank value in Date taken field in Windows Explorer - Windows 8.1 Gold
304467303	3044673: Photos taken by certain Android devices show blank value in Date taken field in Windows Explorer - Windows 8.1 Gold (x64)
304467307	3044673: Photos taken by certain Android devices show blank value in Date taken field in Windows Explorer - Windows 8 Gold
304467311	3044673: Photos taken by certain Android devices show blank value in Date taken field in Windows Explorer - Windows 8 Gold (x64)
304555701	UPDATE: Microsoft .NET Framework 4.6 Available - Windows Vista SP2 / Windows 7 SP1 / Windows 8 / Windows 8.1 / Windows Server 2008 R2 SP1 / Windows Server 2008 SP2 / Windows Server 2012 / Windows Server 2012 R2
304563403	3045634: You cannot make a PPP connection after you reconnect a PLC device in Windows 8.1 or Windows 8 - Windows 8.1 Gold (x64)
304563405	3045634: You cannot make a PPP connection after you reconnect a PLC device in Windows 8.1 or Windows 8 - Windows 8.1 Gold
304564503	3045645: Update to force a UAC prompt when a customized .sdb file is created in Windows - Windows 7 SP1 (x64)
304564505	3045645: Update to force a UAC prompt when a customized .sdb file is created in Windows - Windows 8 Gold
304564507	3045645: Update to force a UAC prompt when a customized .sdb file is created in Windows - Windows 8 Gold (x64)

304564509	3045645: Update to force a UAC prompt when a customized .sdb file is created in Windows - Windows 7 SP1
304571701	3045717: Narrator does not stop reading when you press Ctrl key in Windows - Windows 8.1 Gold
304571705	3045717: Narrator does not stop reading when you press Ctrl key in Windows - Windows 8.1 Gold (x64)
304571901	3045719: Microsoft Project Siena crashes when you use galleries in the application in Windows - Windows 8.1 Gold
304571905	3045719: Microsoft Project Siena crashes when you use galleries in the application in Windows - Windows 8.1 Gold (x64)
304575503	3045755: Security Advisory: Update to improve PKU2U authentication - Windows 8.1 Gold
304575505	3045755: Security Advisory: Update to improve PKU2U authentication - Windows 8.1 Gold (x64)
304599205	3045992: "Description cannot be found" error in event logs in Event Viewer in Windows Server 2012 R2 or Windows Server 2012 - Windows 8 Gold
304599211	3045992: "Description cannot be found" error in event logs in Event Viewer in Windows Server 2012 R2 or Windows Server 2012 - Windows 8 Gold (x64)
304601503	3046015: Security Advisory: Vulnerability in Schannel Could Allow Security Feature Bypass - Disable Workaround
304648001	3046480: Update helps to determine whether to migrate the .NET Framework 1.1 when you upgrade Windows 8.1 or Windows 7 - Windows 8.1 Gold (x64)
304648003	3046480: Update helps to determine whether to migrate the .NET Framework 1.1 when you upgrade Windows 8.1 or Windows 7 - Windows 8.1 Gold
304648005	3046480: Update helps to determine whether to migrate the .NET Framework 1.1 when you upgrade Windows 8.1 or Windows 7 - Windows 7 Gold/SP1 (x64)
304648007	3046480: Update helps to determine whether to migrate the .NET Framework 1.1 when you upgrade Windows 8.1 or Windows 7 - Windows 7 Gold/SP1
304673701	3046737: "Paired" text is not translated correctly in Korean when you disconnect a paired Bluetooth device in Windows - Windows 8.1 Gold
304673703	3046737: "Paired" text is not translated correctly in Korean when you disconnect a paired Bluetooth device in Windows - Windows 8.1 Gold (x64)
304725401	3047254: Stop error 0x0000009F when you use the Bluetooth Hands-Free Audio and Call Control HID Enumerator driver in Windows 8.1 - Windows 8.1 Gold

304725403	3047254: Stop error 0x0000009F when you use the Bluetooth Hands-Free Audio and Call Control HID Enumerator driver in Windows 8.1 - Windows 8.1 Gold (x64)
304804303	3048043: Screen flickers or becomes blank when you drag tiles on the Start screen in Windows - Windows 8.1 Gold
304804305	3048043: Screen flickers or becomes blank when you drag tiles on the Start screen in Windows - Windows 8.1 Gold (x64)
304876105	3048761: Information or messages are not updated automatically in an application in Windows 7 or Windows Server 2008 R2 - Windows 7 SP1 (x64)
304876107	3048761: Information or messages are not updated automatically in an application in Windows 7 or Windows Server 2008 R2 - Windows 7 SP1
305386301	3053863: Windows 8.1 can't discover Samsung TV as wireless display device - Windows 8.1 Gold
305386303	3053863: Windows 8.1 can't discover Samsung TV as wireless display device - Windows 8.1 Gold (x64)
305394601	3053946: "0x00000113" Stop error when you wake a computer from sleep mode in Windows 8.1 - Windows 8.1 Gold (x64)
305416903	3054169: Update to add more information to minidump files that helps OCA servers categorize failures correctly in Windows - Windows 8.1 Gold
305416905	3054169: Update to add more information to minidump files that helps OCA servers categorize failures correctly in Windows - Windows 8.1 Gold (x64)
305425603	3054256: Reliability improvements for Windows 8.1 - Windows 8.1 Gold (x64)
305425605	3054256: Reliability improvements for Windows 8.1 - Windows 8.1 Gold
305446401	3054464: Applications that use the AddEntry method may crash in Windows - Windows 8.1 Gold
305446405	3054464: Applications that use the AddEntry method may crash in Windows - Windows 8.1 Gold (x64)
305447601	3054476: Update for stream.sys driver-based applications in Windows 7 or Windows Server 2008 R2 - Windows 7 SP1
305447605	3054476: Update for stream.sys driver-based applications in Windows 7 or Windows Server 2008 R2 - Windows 7 SP1 (x64)
305532301	3055323: Update to enable a security feature in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 Gold (x64)
305532303	3055323: Update to enable a security feature in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 Gold
305534307	3055343: Update for Windows 8.1 (KB3055343) - Windows 8.1 (V2.0)
305534309	3055343: Update for Windows 8.1 for x64-based Systems (KB3055343) - Windows 8.1 (x64) (V2.0)

305634701	3056347: Location feature is not turned off after you enable "Turn off location" policy setting in Windows RT 8.1 or Windows 8.1 - Windows 8.1 Gold
305634703	3056347: Location feature is not turned off after you enable "Turn off location" policy setting in Windows RT 8.1 or Windows 8.1 - Windows 8.1 Gold (x64)
305715413	3057154: Security advisory: Update to harden use of DES encryption - Windows Vista SP2 (x64)
305715427	3057154: Security advisory: Update to harden use of DES encryption - Windows Vista SP2
306038301	3060383: Decimal symbol and digit grouping symbol are incorrect for the Swiss language locale in Windows - Windows 8 Gold (x64)
306038305	3060383: Decimal symbol and digit grouping symbol are incorrect for the Swiss language locale in Windows - Windows 8 Gold
306074601	3060746: You can't open the "Devices" menu in PC Settings in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 Gold
306074605	3060746: You can't open the "Devices" menu in PC Settings in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 Gold (x64)
306079301	3060793: "0x0000001E" or "0x00000133" Stop error when you transfer data through a USB-based RNDIS device on Windows - Windows 8.1 Gold (x64)
306079305	3060793: "0x0000001E" or "0x00000133" Stop error when you transfer data through a USB-based RNDIS device on Windows - Windows 8.1 Gold
306149301	3061493: Update enables magstripe drivers to support new devices in Windows 8.1 or Windows RT 8.1 - Windows 8.1 Gold
306149303	3061493: Update enables magstripe drivers to support new devices in Windows 8.1 or Windows RT 8.1 - Windows 8.1 Gold (x64)
306259101	3062591: Security advisory: Local Administrator Password Solution (LAPS) now available - GPO CSE
306259103	3062591: Security advisory: Local Administrator Password Solution (LAPS) now available - GPO CSE (x64)
306276001	3062760: Security advisory: Update for vulnerability in Juniper Networks Windows In-Box Junos Pulse client - Windows 8.1 Gold (x64)
306276003	3062760: Security advisory: Update for vulnerability in Juniper Networks Windows In-Box Junos Pulse client - Windows 8.1 Gold
306310901	3063109: Hyper-V integration components update for Windows virtual machines that are running on a Windows 10-based host - Windows 8.1 - KB3063109
306310909	3063109: Hyper-V integration components update for Windows virtual machines that are running on a Windows 10-based host - Windows 7 SP1 - KB3063109 (x64)

306310911	3063109: Hyper-V integration components update for Windows virtual machines that are running on a Windows 10-based host - Windows 7 SP1 - KB3063109
306310913	3063109: Hyper-V integration components update for Windows virtual machines that are running on a Windows 10-based host - Windows 8.1 - KB3063109 (x64)
306384303	3063843: System takes too long time to log on to a computer because of large numbers of WNF state name registrations in Windows - Windows 8.1 Gold (x64)
306384305	3063843: System takes too long time to log on to a computer because of large numbers of WNF state name registrations in Windows - Windows 8.1 Gold
306405901	3064059: Explorer.exe process crashes after File History item in Control Panel is opened in Windows 8.1 - Windows 8.1 Gold
306405903	3064059: Explorer.exe process crashes after File History item in Control Panel is opened in Windows 8.1 - Windows 8.1 Gold (x64)
306420901	3064209: Microcode update for Intel processors in Windows - Windows 8 Gold
306420903	3064209: Microcode update for Intel processors in Windows - Windows 7 SP1
306420905	3064209: Microcode update for Intel processors in Windows - Windows 7 SP1 (x64)
306420907	3064209: Microcode update for Intel processors in Windows - Windows 8 Gold (x64)
306420915	3064209: Microcode update for Intel processors in Windows - Windows 8.1 Gold
306420917	3064209: Microcode update for Intel processors in Windows - Windows 8.1 Gold (x64)
307201901	3072019: "Try again" error occurs and Bluetooth device cannot connect to computer in Windows 8.1 or Windows RT 8.1 - Windows 8.1 Gold (x64)
307201903	3072019: "Try again" error occurs and Bluetooth device cannot connect to computer in Windows 8.1 or Windows RT 8.1 - Windows 8.1 Gold
307771547	3077715: Cumulative time zone update for Windows operating systems - Windows 8.1 - KB3077715 (x64)
307771551	3077715: Cumulative time zone update for Windows operating systems - Windows 8.1 - KB3077715
307840503	3078405: "0x0000004A" or "0x0000009F" Stop error occurs in Windows 8.1 - Windows 8.1 Gold - KB3078405
307840511	3078405: "0x0000004A" or "0x0000009F" Stop error occurs in Windows 8.1 - Windows 8.1 Gold - KB3078405 (x64)
307866705	3078667: System malfunction because memory leak occurs in dwm.exe in Windows 7 or Windows Server 2008 R2 - Windows 7 SP1 (x64)

307866707	3078667: System malfunction because memory leak occurs in dwm.exe in Windows 7 or Windows Server 2008 R2 - Windows 7 SP1
307867603	3078676: Event 1530 is logged and ProfSvc leaks paged pool memory and handles in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 Gold (x64)
307867605	3078676: Event 1530 is logged and ProfSvc leaks paged pool memory and handles in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 Gold
308004201	3080042: CHM file freezes when you enter characters in Search box on the Index tab in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 Gold (x64)
308004203	3080042: CHM file freezes when you enter characters in Search box on the Index tab in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 Gold
308007901	3080079: Update to add RDS support for TLS 1.1 and TLS 1.2 in Windows 7 or Windows Server 2008 R2 - Windows 7 SP1 (x64)
308007903	3080079: Update to add RDS support for TLS 1.1 and TLS 1.2 in Windows 7 or Windows Server 2008 R2 - Windows 7 SP1
308014905	3080149: Update for customer experience and diagnostic telemetry - Windows 8.1 Gold
308014913	3080149: Update for customer experience and diagnostic telemetry - Windows 8.1 Gold (x64)
308045701	3080457: Windows Communications Apps update f or WSUS for Windows 8.1 - Windows 8.1 Gold
308045703	3080457: Windows Communications Apps update f or WSUS for Windows 8.1 - Windows 8.1 Gold (x64)
308080001	3080800: "Access violation (c0000005)" error if the NcdAutoSetup service crashes in Windows 8.1 or Windows RT 8.1 - Windows 8.1 Gold
308080003	3080800: "Access violation (c0000005)" error if the NcdAutoSetup service crashes in Windows 8.1 or Windows RT 8.1 - Windows 8.1 Gold (x64)
308139701	3081397: Bing Finance app update for WSUS for Windows 8.1 - Windows 8.1 Gold (x64)
308139703	3081397: Bing Finance app update for WSUS for Windows 8.1 - Windows 8.1 Gold
308139801	3081398: Bing Travel app update for WSUS for Windows 8.1 - Windows 8.1 Gold
308139803	3081398: Bing Travel app update for WSUS for Windows 8.1 - Windows 8.1 Gold (x64)
308139901	3081399: Bing Sports app update for WSUS for Windows 8.1 - Windows 8.1 Gold
308139903	3081399: Bing Sports app update for WSUS for Windows 8.1 - Windows 8.1 Gold (x64)

308140101	3081401: Bing News app update for WSUS for Windows 8.1 - Windows 8.1 Gold
308140103	3081401: Bing News app update for WSUS for Windows 8.1 - Windows 8.1 Gold (x64)
308140201	3081402: Bing Maps app update for WSUS for Windows 8.1 - Windows 8.1 Gold
308140203	3081402: Bing Maps app update for WSUS for Windows 8.1 - Windows 8.1 Gold (x64)
308140301	3081403: Bing Health & Fitness app update for WSUS for Windows 8.1 - Windows 8.1 Gold
308140303	3081403: Bing Health & Fitness app update for WSUS for Windows 8.1 - Windows 8.1 Gold (x64)
308140501	3081405: Bing Weather app update for WSUS for Windows 8.1 - Windows 8.1 Gold
308140503	3081405: Bing Weather app update for WSUS for Windows 8.1 - Windows 8.1 Gold (x64)
308195401	3081954: Update for Work Folders improvements in Windows 7 SP1 - Windows 7 SP1 - KB3081954 (x64)
308195403	3081954: Update for Work Folders improvements in Windows 7 SP1 - Windows 7 SP1 - KB3081954
308235303	3082353: Windows 8.1 or Windows Server 2012 R2 hosts crash when they set up IPSec tunnel - Windows 8.1 Gold (x64)
308235305	3082353: Windows 8.1 or Windows Server 2012 R2 hosts crash when they set up IPSec tunnel - Windows 8.1 Gold
308399209	3083992: Security advisory: Update to Improve AppLocker Publisher Rule Enforcement - Windows 8 Gold (x64)
308399215	3083992: Security advisory: Update to Improve AppLocker Publisher Rule Enforcement - Windows 8 Gold
308490501	3084905: TPM lockout occurs unexpectedly in Windows 8.1 or Windows RT 8.1 - Windows 8.1 Gold (x64) (V2.0)
308490503	3084905: TPM lockout occurs unexpectedly in Windows 8.1 or Windows RT 8.1 - Windows 8.1 Gold (V2.0)
308490505	3084905: TPM lockout occurs unexpectedly in Windows 8.1 or Windows RT 8.1 - Windows Server 2012 R2 Gold (x64) (V2.0)
308625503	MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows 8.1 Gold - KB3086255
308625507	MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows 8 Gold - KB3086255 (x64)
308625511	MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows 8 Gold - KB3086255
308625515	MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows 7 SP1 - KB3086255

308625517	MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows Vista SP2 - KB3086255
308625521	MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows 7 SP1 - KB3086255 (x64)
308625523	MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows 8.1 Gold - KB3086255 (x64)
308625525	MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution - Windows Vista SP2 - KB3086255 (x64)
308713701	3087137: Gradient rendering issue when an application has nested transformed geometries in Windows 8.1 - Windows 8.1 Gold
308713705	3087137: Gradient rendering issue when an application has nested transformed geometries in Windows 8.1 - Windows 8.1 Gold (x64)
308787301	3087873: "0x0000007E" Stop error after you install hotfix 2990941 in Windows 7 SP1 or Windows Server 2008 R2 SP1 - Windows 7 SP1 - KB3087873
308787303	3087873: "0x0000007E" Stop error after you install hotfix 2990941 in Windows 7 SP1 or Windows Server 2008 R2 SP1 - Windows 7 SP1 / Windows Server 2008 R2 SP1 - KB3087873 (x64)
309129703	3091297: You can't logon to an AD FS server from a Windows Store app on a Windows 8.1 or Windows RT 8.1 device - Windows 8.1 Gold - KB3091297 (x64)
309129705	3091297: You can't logon to an AD FS server from a Windows Store app on a Windows 8.1 or Windows RT 8.1 device - Windows 8.1 Gold - KB3091297
309262721	3092627: Update to fix Windows or application freezes after you install security update 3076895 - Windows 8 Gold (x64)
309262723	3092627: Update to fix Windows or application freezes after you install security update 3076895 - Windows Vista SP2 (x64)
309262725	3092627: Update to fix Windows or application freezes after you install security update 3076895 - Windows 8 Gold
309262727	3092627: Update to fix Windows or application freezes after you install security update 3076895 - Windows Vista SP2
309350301	3093503: Time zone and daylight saving time changes for Democratic People's Republic of Korea, Turkey, and Fiji in Windows - Windows 7 SP1 / Windows Server 2008 R2 SP1 (x64) (V3.0) (Superseded)
309350303	3093503: Time zone and daylight saving time changes for Democratic People's Republic of Korea, Turkey, and Fiji in Windows - Windows Vista SP2 / Windows Server 2008 SP2 (x64) (V3.0)(Superseded)
309350305	3093503: Time zone and daylight saving time changes for Democratic People's Republic of Korea, Turkey, and Fiji in Windows - Windows 8.1 Gold / Windows Server 2012 R2 (x64) (V6.0)(Superseded)
309350307	3093503: Time zone and daylight saving time changes for Democratic People's Republic of Korea, Turkey, and Fiji in Windows - Windows 8 Gold / Windows 2012 Gold (x64) (V3.0)(Superseded)

309350311	3093503: Time zone and daylight saving time changes for Democratic People's Republic of Korea, Turkey, and Fiji in Windows - Windows 8.1 Gold (V6.0)(Superseded)
309350313	3093503: Time zone and daylight saving time changes for Democratic People's Republic of Korea, Turkey, and Fiji in Windows - Windows 8 Gold (V3.0)(Superseded)
309350315	3093503: Time zone and daylight saving time changes for Democratic People's Republic of Korea, Turkey, and Fiji in Windows - Windows Vista SP2 / Windows Server 2008 SP2 (V3.0)(Superseded)
309350317	3093503: Time zone and daylight saving time changes for Democratic People's Republic of Korea, Turkey, and Fiji in Windows - Windows 7 SP1 (V3.0)(Superseded)
309510801	3095108: Updated APN database entry for Transatel (France, Worldwide) network for Windows 8.1 and Windows 8 - Windows 8 Gold - KB3095108 (x64)
309510803	3095108: Updated APN database entry for Transatel (France, Worldwide) network for Windows 8.1 and Windows 8 - Windows 8 Gold - KB3095108
309796605	3097966: Inadvertently Disclosed Digital Certificates Could Allow Spoofing - Windows 8 Gold - KB3097966 (x64)
309796613	3097966: Inadvertently Disclosed Digital Certificates Could Allow Spoofing - Windows Vista SP2 - KB3097966 (x64)
309796619	3097966: Inadvertently Disclosed Digital Certificates Could Allow Spoofing - Windows Vista SP2 - KB3097966
309796625	3097966: Inadvertently Disclosed Digital Certificates Could Allow Spoofing - Windows 8 Gold - KB3097966
310047303	3100473: DNS records get deleted when you delete the scope on a Windows Server 2012 R2-based DHCP server - Windows 8.1 - KB3100473 (x64)
310047305	3100473: DNS records get deleted when you delete the scope on a Windows Server 2012 R2-based DHCP server - Windows 8.1 - KB3100473
310242923	3102429: Update that supports Azerbaijani Manat and Georgian Lari currency symbols in Windows - Windows 8.1 Gold - KB3102429 (x64) (V2.0)
310242925	3102429: Update that supports Azerbaijani Manat and Georgian Lari currency symbols in Windows - Windows 7 SP1 - KB3102429 (x64) (V2.0)
310242927	3102429: Update that supports Azerbaijani Manat and Georgian Lari currency symbols in Windows - Windows 7 SP1 - KB3102429 (V2.0)
310242929	3102429: Update that supports Azerbaijani Manat and Georgian Lari currency symbols in Windows - Windows 8.1 Gold - KB3102429 (V2.0)
310243601	3102436: UPDATE: Microsoft .NET Framework 4.6.1 Available - Windows 7 SP1 / Windows 8 Gold / Windows 8.1 Gold / Windows 2008 R2 SP1 / Windows 2008 SP2 / Windows 2012 Gold / Windows 2012 R2 Gold

310243603	3102436: UPDATE: Microsoft .NET Framework 4.6.1 Available - Windows 10
310361613	3103616: WMI query doesn't work in Windows Server 2012 R2 or Windows Server 2012 - Windows 8.1 - KB3103616 (x64)
310361623	3103616: WMI query doesn't work in Windows Server 2012 R2 or Windows Server 2012 - Windows 8.1 - KB3103616
310369601	3103696: Update for USB Type-C billboard support and Kingston thumb drive is enumerated incorrectly in Windows - Windows 8.1 Gold - KB3103696 (x64)
310369605	3103696: Update for USB Type-C billboard support and Kingston thumb drive is enumerated incorrectly in Windows - Windows 8.1 Gold - KB3103696
310370911	3103709: Windows Server 2012 R2-based domain controller update - Windows 8.1 - KB3103709
310370913	3103709: Windows Server 2012 R2-based domain controller update - Windows 8.1 - KB3103709 (x64)
310799801	3107998: Remove Lenovo USB Blocker version 1.0.0.37 to avoid a system crash - Windows 8 Gold - KB3107998
310799809	3107998: Remove Lenovo USB Blocker version 1.0.0.37 to avoid a system crash - Windows 8 Gold - KB3107998 (x64)
310860401	3108638: Security advisory: Description of the security update for Windows Hyper-V - Windows 8.1 Gold - KB3108604 (x64)
310860403	3108638: Security advisory: Description of the security update for Windows Hyper-V - Windows 8 Gold - KB3108604 (x64)
310985305	3109853: Security advisory: Update to improve TLS session resumption interoperability - Windows 8 Gold - KB3109853 (x64)
310985307	3109853: Security advisory: Update to improve TLS session resumption interoperability - Windows 8 Gold - KB3109853
310997601	3109976: Texas Instruments xHCI USB controllers may encounter a hardware issue on large data transfers in Windows 8.1 - Windows 8.1 - KB3109976 (x64)
310997603	3109976: Texas Instruments xHCI USB controllers may encounter a hardware issue on large data transfers in Windows 8.1 - Windows 8.1 - KB3109976
311214807	3112148: cumulative time zone update for Windows operating systems - Windows 8 Gold - KB3112148 (x64)
311214811	3112148: cumulative time zone update for Windows operating systems - Windows 8 Gold - KB3112148
311840105	3118401: Update for Universal C Runtime in Windows - Windows Vista SP2 - KB3118401 (x64)
311840117	3118401: Update for Universal C Runtime in Windows - Windows Vista SP2 - KB3118401

311988401	3119884: Security advisory: Inadvertently Disclosed Digital Certificates Could Allow Spoofing - Windows Vista SP2 / Windows Server 2008 SP2 / Windows 7 SP1 / Windows Server 2008 R2 SP1 / Windows 8 / Windows Server 2012 / Windows 8.1 / Windows Server 2012
312126103	3121261: System fails back to a host copy instead of an array copy or storages go down after LUN reset in Windows Server 2012 R2 - Windows 8.1 Gold - KB3121261 (x64)
312126105	3121261: System fails back to a host copy instead of an array copy or storages go down after LUN reset in Windows Server 2012 R2 - Windows 8.1 Gold - KB3121261
312347909	3123479: Security advisory: Deprecation of SHA-1 hashing algorithm for Microsoft root certificate program - Windows 8 Gold - KB3123479
312347919	3123479: Security advisory: Deprecation of SHA-1 hashing algorithm for Microsoft root certificate program - Windows 8 Gold - KB3123479 (x64)
312386201	3123862: Updated capabilities to upgrade Windows 8.1 and Windows 7 - Windows 7 SP1 - KB3123862
312386203	3123862: Updated capabilities to upgrade Windows 8.1 and Windows 7 - Windows 8.1 - KB3123862 (x64)
312386205	3123862: Updated capabilities to upgrade Windows 8.1 and Windows 7 - Windows 7 SP1 - KB3123862 (x64)
312386207	3123862: Updated capabilities to upgrade Windows 8.1 and Windows 7 - Windows 8.1 - KB3123862
312557401	3125574: Convenience rollup update for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - KB3125574
312557403	3125574: Convenience rollup update for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - KB3125574 (x64)
312557405	3125574: Convenience rollup update for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows Server 2008 R2 SP1 - KB3125574 (x64)
312603001	3126030: Incorrect log in Event Viewer after you install an antivirus software in Windows 8.1 - Windows 8.1 Gold - KB3126030
312603003	3126030: Incorrect log in Event Viewer after you install an antivirus software in Windows 8.1 - Windows 8.1 Gold - KB3126030 (x64)
312604101	MS16-014: Security Update for Windows Vista - Windows Vista SP2 - KB3126041
312604105	MS16-014: Security Update for Windows 8.1 - Windows 8.1 Gold - KB3126041
312604107	MS16-014: Security Update for Windows 8.1 - Windows 8.1 Gold - KB3126041 (x64)
312604111	MS16-014: Security Update for Windows Vista - Windows Vista SP2 - KB3126041 (x64)
312721901	MS16-019: Security Update for .NET Framework to Address Denial of Service - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB3127219

312721903	MS16-019: Security Update for .NET Framework to Address Denial of Service - Windows Server 2008 SP2 / Windows Vista SP2 - .NET Framework 2.0 SP2 - KB3127219 (x64)
312865001	3128650: Access to COM+ role-based security is denied in Windows Server 2012 R2 - Windows 8.1 Gold - KB3128650 (x64)
312865005	3128650: Access to COM+ role-based security is denied in Windows Server 2012 R2 - Windows 8.1 Gold - KB3128650
313208003	3132080: The logon process hangs at the "Welcome" screen or the "Please wait for the User Profile Service" error message window - Windows 8.1 Gold - KB3132080 (x64)
313208005	3132080: The logon process hangs at the "Welcome" screen or the "Please wait for the User Profile Service" error message window - Windows 8.1 Gold - KB3132080
313237205	3132372: Security advisory: Update for vulnerabilities in Adobe Flash Player in Internet Explorer and Microsoft Edge - Windows 8 Gold - KB3132372(Superseded)
313237207	3132372: Security advisory: Update for vulnerabilities in Adobe Flash Player in Internet Explorer and Microsoft Edge - Windows 8 Gold - KB3132372 (x64)(Superseded)
313343121	3133431: Security advisory: Update for vulnerabilities in Adobe Flash Player in Internet Explorer and Microsoft Edge - Windows 8 Gold - KB3133431
313343123	3133431: Security advisory: Update for vulnerabilities in Adobe Flash Player in Internet Explorer and Microsoft Edge - Windows 8 Gold - KB3133431 (x64)
313369001	3133690: Update to add Discrete Device Assignment support for Azure that runs on Windows Server 2012 R2-based guest VMs - Windows 8.1 - KB3133690 (x64)
313397701	3133977: BitLocker can't encrypt drives and the service crashes in svchost.exe process in Windows 7 or Windows Server 2008 R2 - Windows 7 SP1 - KB3133977
313397703	3133977: BitLocker can't encrypt drives and the service crashes in svchost.exe process in Windows 7 or Windows Server 2008 R2 - Windows 7 SP1 - KB3133977 (x64)
313481201	3134812: You can't change settings from FSRM GUI in Windows Server 2012 R2 - Windows 8.1 Gold - KB3134812
313481205	3134812: You can't change settings from FSRM GUI in Windows Server 2012 R2 - Windows 8.1 Gold - KB3134812 (x64)
313706105	3137061: Windows Azure VMs don't recover from a network outage and data corruption issues occur - Windows 7 SP1 - KB3137061 (x64)
313706109	3137061: Windows Azure VMs don't recover from a network outage and data corruption issues occur - Windows 7 SP1 - KB3137061

313772801	3137728: VSS restore fails when you use ResyncLuns VSS API in Windows Server 2012 R2-based failover cluster - Windows 8.1 - KB3137728 (x64)
313772803	3137728: VSS restore fails when you use ResyncLuns VSS API in Windows Server 2012 R2-based failover cluster - Windows 8.1 - KB3137728
313837835	3138378: Update for Journal.dll binary in Windows - Windows 8.1 - KB3138378 (x64)
313837837	3138378: Update for Journal.dll binary in Windows - Windows 7 SP1 - KB3138378
313837839	3138378: Update for Journal.dll binary in Windows - Windows 7 SP1 - KB3138378 (x64)
313837847	3138378: Update for Journal.dll binary in Windows - Windows Vista SP2 - KB3138378
313837849	3138378: Update for Journal.dll binary in Windows - Windows 8.1 - KB3138378
313837851	3138378: Update for Journal.dll binary in Windows - Windows Vista SP2 - KB3138378 (x64)
313860201	3138602: "File contents" option is always selectable, Start screen becomes blank, or computer freezes when startup in Windows 8.1 - Windows 8.1 - KB3138602 (x64)
313860205	3138602: "File contents" option is always selectable, Start screen becomes blank, or computer freezes when startup in Windows 8.1 - Windows 8.1 - KB3138602
313861201	3138612: Windows Update Client for Windows 7 and Windows Server 2008 R2 - Windows 7 SP1 - KB3138612
313861203	3138612: Windows Update Client for Windows 7 and Windows Server 2008 R2 - Windows 7 SP1 - KB3138612 (x64)
313992129	3139921: "No computer account for trust" error when you change domain account password in Windows - Windows Vista SP2 - KB3139921 (x64)
313992131	3139921: "No computer account for trust" error when you change domain account password in Windows - Windows Vista SP2 - KB3139921
314018501	3140185: WAU update for Windows 8.1 - Windows 8.1 - KB3140185
314018503	3140185: WAU update for Windows 8.1 - Windows 8.1 - KB3140185 (x64)
314021901	3140219: "0x00000133" Stop error after you install hotfix 3061460 in Windows Server 2012 R2 - Windows 8.1 - KB3140219 (x64)
314021903	3140219: "0x00000133" Stop error after you install hotfix 3061460 in Windows Server 2012 R2 - Windows 8.1 - KB3140219
314023401	3140234: "0x0000009F" Stop error when a Windows VPN client computer is shutdown with an active L2TP VPN connection - Windows 8.1 - KB3140234 (x64)

314023403	3140234: "0x0000009F" Stop error when a Windows VPN client computer is shutdown with an active L2TP VPN connection - Windows 8.1 - KB3140234
314024519	3140245: A new registry key enables TLS 1.1 and TLS 1.2 to default secure protocols in WinHTTP in Windows - Windows 7 SP1 - KB3140245
314024521	3140245: A new registry key enables TLS 1.1 and TLS 1.2 to default secure protocols in WinHTTP in Windows - Windows 7 SP1 - KB3140245 (x64)
314538407	3145384: MinDiffAreaFileSize registry value limit is increased from 3 GB to 50 GB in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 - KB3145384 (x64)
314538411	3145384: MinDiffAreaFileSize registry value limit is increased from 3 GB to 50 GB in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 - KB3145384
314660413	3146604: WMI service crashes randomly in Windows Server 2012 R2 or Windows Server 2012 - Windows 8.1 - KB3146604
314660415	3146604: WMI service crashes randomly in Windows Server 2012 R2 or Windows Server 2012 - Windows 8.1 - KB3146604 (x64)
314675107	3146751: "Logon is not possible" error or a temporary file is created when you log on App-V in Windows Server 2012 R2 - Windows 8.1 - KB3146571 (x64)
314675111	3146751: "Logon is not possible" error or a temporary file is created when you log on App-V in Windows Server 2012 R2 - Windows 8.1 - KB3146571
314707101	3147071: Connection to Oracle database fails when you use Microsoft ODBC or OLE DB Driver for Oracle or Microsoft DTC in Windows - Windows Vista SP2 - KB3147071 (x64)
314707103	3147071: Connection to Oracle database fails when you use Microsoft ODBC or OLE DB Driver for Oracle or Microsoft DTC in Windows - Windows 7 SP1 - KB3147071 (x64)
314707109	3147071: Connection to Oracle database fails when you use Microsoft ODBC or OLE DB Driver for Oracle or Microsoft DTC in Windows - Windows 8.1 - KB3147071 (x64)
314707117	3147071: Connection to Oracle database fails when you use Microsoft ODBC or OLE DB Driver for Oracle or Microsoft DTC in Windows - Windows 8.1 - KB3147071
314707119	3147071: Connection to Oracle database fails when you use Microsoft ODBC or OLE DB Driver for Oracle or Microsoft DTC in Windows - Windows 7 SP1 - KB3147071
314707121	3147071: Connection to Oracle database fails when you use Microsoft ODBC or OLE DB Driver for Oracle or Microsoft DTC in Windows - Windows Vista SP2 - KB3147071

314915707	3149157: Reliability and scalability improvements in TCP/IP for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - KB3149157 (x64)
314915711	3149157: Reliability and scalability improvements in TCP/IP for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - KB3149157
315051301	3150513: Compatibility Update for Windows - Windows 8 (x64)
315051303	3150513: Compatibility Update for Windows - Windows 8.1 (x64)
315051305	3150513: Compatibility Update for Windows - Windows 8.1
315051307	3150513: Compatibility Update for Windows - Windows 8
315051309	3150513: Compatibility Update for Windows - Windows 7 SP1
315051311	3150513: Compatibility Update for Windows - Windows 7 SP1 (x64)
315051313	3150513: Compatibility Update for Windows - Windows 7 SP1
315051315	3150513: Compatibility Update for Windows - Windows 7 SP1 (x64)
316110201	3161102: Update for Windows Journal component removal - Windows 7 SP1 - KB3161102
316110203	3161102: Update for Windows Journal component removal - Windows 7 SP1 - KB3161102 (x64)
316110205	3161102: Update for Windows Journal component removal - Windows 8.1 - KB3161102
316110207	3161102: Update for Windows Journal component removal - Windows 8.1 - KB3161102 (x64)
317073501	3170735: Update for Windows Journal - Windows 7 SP1 - KB3170735
317073505	3170735: Update for Windows Journal - Windows 7 SP1 - KB3170735 (x64)
317260501	3172605: Update rollup for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - KB3172605
317260505	3172605: Update rollup for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - KB3172605 (x64)
317261401	3172614: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - Windows 8.1 - KB3172614 (x64)
317261405	3172614: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - Windows 8.1 - KB3172614
317304009	3173040: Windows 8.1 and Windows 7 SP1 end of free upgrade offer notification - Windows 7 SP1 - KB3173040 (V2.0)
317304011	3173040: Windows 8.1 and Windows 7 SP1 end of free upgrade offer notification - Windows 7 SP1 - KB3173040 (x64) (V2.0)
317304013	3173040: Windows 8.1 and Windows 7 SP1 end of free upgrade offer notification - Windows 8.1 - KB3173040 (x64) (V2.0)
317304015	3173040: Windows 8.1 and Windows 7 SP1 end of free upgrade offer notification - Windows 8.1 - KB3173040 (V2.0)
317464401	3174644: Security advisory: Updated support for Diffie-Hellman Key Exchange - Set Diffie-Hellman Modulus Size - KB3174644

317464403	3174644: Security advisory: Updated support for Diffie-Hellman Key Exchange - Reset Diffie-Hellman Modulus Size to Default - KB3174644
317957301	3179573: Update rollup for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - KB3179573
317957303	3179573: Update rollup for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - KB3179573 (x64)
317957403	3179574: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - Windows 8.1 - KB3179574 (x64)
317957405	3179574: Update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - Windows 8.1 - KB3179574
318198801	3181988: SFC integrity scan reports and fixes an error in the usbhub.sys.mui file in Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - KB3181988
318198805	3181988: SFC integrity scan reports and fixes an error in the usbhub.sys.mui file in Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - KB3181988 (x64)
318414301	3184143: Remove software related to the Windows 10 free upgrade offer - Windows 7 - KB3184143 (x64)
318414303	3184143: Remove software related to the Windows 10 free upgrade offer - Windows 7 - KB3184143
318414305	3184143: Remove software related to the Windows 10 free upgrade offer - Windows 8.1 - KB3184143 (x64)
318414307	3184143: Remove software related to the Windows 10 free upgrade offer - Windows 8.1 - KB3184143
318566201	3185662: Windows Journal update for Windows Vista SP2 - Windows Vista SP2 - KB3185662 (x64)
318566203	3185662: Windows Journal update for Windows Vista SP2 - Windows Vista SP2 - KB3185662
318649701	3186497: UPDATE: Microsoft .NET Framework 4.7 Available - Windows 7 SP1 / Windows 8.1 / Windows 2008 R2 SP1 / Windows 2012 / Windows 2012 R2 / Windows 10 / Windows Server 2016
319120301	MS16-120, MS16-123: Security Update for Microsoft Graphics Component - Windows Server 2008 SP2 / Windows Vista SP2 - KB3191203
319120303	MS16-120, MS16-123: Security Update for Microsoft Graphics Component - Windows Server 2008 SP2 / Windows Vista SP2 - KB3191203 (x64)
319156403	3191564: Update for Windows Management Framework 5.1 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - KB3191564 (x64)
319156405	3191564: Update for Windows Management Framework 5.1 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - KB3191564
319156601	3191566: Update for Windows Management Framework 5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - KB3191566

319156603	3191566: Update for Windows Management Framework 5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - KB3191566 (x64)
319239101	MS16-101, MS16-118, MS16-120, MS16-122, MS16-123, MS16-124, MS16-126: Security only quality update - Security Only - Windows 7 SP1 - KB3192391
319239103	MS16-101, MS16-118, MS16-120, MS16-122, MS16-123, MS16-124, MS16-126: Security only quality update - Security Only - Windows 7 SP1 / Windows Server 2008 R2 SP1 - KB3192391 (x64)
319239201	MS16-101, MS16-118, MS16-120, MS16-122, MS16-123, MS16-124: Security only quality update - Security Only - Windows 8.1 - KB3192392
319239203	MS16-101, MS16-118, MS16-120, MS16-122, MS16-123, MS16-124: Security only quality update - Security Only - Windows 8.1 / Windows Server 2012 R2 - KB3192392 (x64)
319786701	MS16-130, MS16-131, MS16-132, MS16-134, MS16-135, MS16-137, MS16-139, MS16-142: Security Update for Microsoft Windows - Security Only - Windows 7 SP1 / Windows Server 2008 R2 SP1 - KB3197867 (x64)
319786703	MS16-130, MS16-131, MS16-132, MS16-134, MS16-135, MS16-137, MS16-139, MS16-142: Security Update for Microsoft Windows - Security Only - Windows 7 SP1 - KB3197867
319787301	MS16-130, MS16-131, MS16-132, MS16-134, MS16-135, MS16-137, MS16-138, MS16-140, MS16-142: Security Update for Microsoft Windows - Security Only - Windows 8.1 / Windows Server 2012 R2 - KB3197873 (x64)
319787303	MS16-130, MS16-131, MS16-132, MS16-134, MS16-135, MS16-137, MS16-138, MS16-140, MS16-142: Security Update for Microsoft Windows - Security Only - Windows 8.1 - KB3197873
320102101	3201021: Update that enables user to set Application Pool to run as Null Virtual Account in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 - KB3201021 (x64)
320102105	3201021: Update that enables user to set Application Pool to run as Null Virtual Account in Windows 8.1 or Windows Server 2012 R2 - Windows 8.1 - KB3201021
320539401	MS16-144, MS16-146, MS16-147, MS16-149, MS16-151, MS16-153: Security Only Quality Update - Security Only - Windows 7 SP1 - KB3205394 (x64)
320539405	MS16-144, MS16-146, MS16-147, MS16-149, MS16-151, MS16-153: Security Only Quality Update - Security Only - Windows 7 SP1 - KB3205394
320540003	MS16-144, MS16-146, MS16-147, MS16-149, MS16-151, MS16-153: Security Only Quality Update - Security Only - Windows 8.1 - KB3205400 (x64)
320540005	MS16-144, MS16-146, MS16-147, MS16-149, MS16-151, MS16-153: Security Only Quality Update - Security Only - Windows 8.1 - KB3205400

321652001	3216520: Preview of the Quality Rollup for the .NET Framework 2.0 SP2, 4.5.2, and 4.6 on Windows Vista SP2 and Windows Server 2008 SP2 - Windows Vista SP2 - KB3216970 (x64)
321652003	3216520: Preview of the Quality Rollup for the .NET Framework 2.0 SP2, 4.5.2, and 4.6 on Windows Vista SP2 and Windows Server 2008 SP2 - Windows Vista SP2 - KB3216970
321652005	3216520: Preview of the Quality Rollup for the .NET Framework 2.0 SP2, 4.5.2, and 4.6 on Windows Vista SP2 and Windows Server 2008 SP2 - Windows Vista SP2 - KB3216973 (x64)
321652007	3216520: Preview of the Quality Rollup for the .NET Framework 2.0 SP2, 4.5.2, and 4.6 on Windows Vista SP2 and Windows Server 2008 SP2 - Windows Vista SP2 - KB3216973
321652011	3216520: Preview of the Quality Rollup for the .NET Framework 2.0 SP2, 4.5.2, and 4.6 on Windows Vista SP2 and Windows Server 2008 SP2 - Windows Vista SP2 - KB3078601 (x64)
321652013	3216520: Preview of the Quality Rollup for the .NET Framework 2.0 SP2, 4.5.2, and 4.6 on Windows Vista SP2 and Windows Server 2008 SP2 - Windows Vista SP2 - KB3078601
321652019	3216520: Preview of the Quality Rollup for the .NET Framework 2.0 SP2, 4.5.2, and 4.6 on Windows Vista SP2 and Windows Server 2008 SP2 - Windows Vista SP2 - KB3217123 (x64)
321652023	3216520: Preview of the Quality Rollup for the .NET Framework 2.0 SP2, 4.5.2, and 4.6 on Windows Vista SP2 and Windows Server 2008 SP2 - Windows Vista SP2 - KB3217123
321787701	3217877: Update for Windows Server 2008 and Windows Vista - Windows Vista SP2 - KB3217877 (x64)
321787705	3217877: Update for Windows Server 2008 and Windows Vista - Windows Vista SP2 - KB3217877
401258303	MS17-011, MS17-013: Security Update for Microsoft Uniscribe - Windows Vista SP2 - KB4012583 (x64)
401258307	MS17-011, MS17-013: Security Update for Microsoft Uniscribe - Windows Vista SP2 - KB4012583
401286405	4012864: DST changes in Windows for Northern Cypress, Mongolia, and Russian Saratov region - Windows Vista SP2 - KB4012864
401456101	MS17-APR: Security Monthly Quality Rollup - Monthly Rollup - Windows Vista SP2 - .NET Framework 2.0 SP2 - KB4014561 (x64)
401456103	MS17-APR: Security Monthly Quality Rollup - Monthly Rollup - Windows Vista SP2 - .NET Framework 2.0 SP2 - KB4014561
401457901	MS17-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4014579 (x64)
401457905	MS17-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4014579
401458103	MS17-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4014581 (x64)

401458105	MS17-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4014581
401458703	MS17-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6.2 - KB4014587 (x64)
401458705	MS17-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6.2 - KB4014587
401458801	MS17-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6.2 - KB4014588 (x64)
401458805	MS17-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6.2 - KB4014588
401459001	MS17-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1 - KB4014590 (x64)
401459005	MS17-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1 - KB4014590
401459103	MS17-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1 - KB4014591 (x64)
401459105	MS17-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1 - KB4014591
401459501	MS17-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4014595 (x64)
401459505	MS17-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4014595
401459903	MS17-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4014599 (x64)
401459905	MS17-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4014599
401465201	MS17-APR: Security update for the libjpeg information disclosure vulnerability in Windows Vista and Windows Server 2008 - Windows Vista SP2 - KB4014652 (x64)
401465207	MS17-APR: Security update for the libjpeg information disclosure vulnerability in Windows Vista and Windows Server 2008 - Windows Vista SP2 - KB4014652
401479303	MS17-APR: Security update for the Microsoft Office remote code execution vulnerability - Windows Vista SP2 - KB4014793 (x64)
401479305	MS17-APR: Security update for the Microsoft Office remote code execution vulnerability - Windows Vista SP2 - KB4014793
401479401	MS17-APR: Security update for the libjpeg information disclosure vulnerability in Windows Vista and Windows Server 2008 - Windows Vista SP2 - KB4014794 (x64)
401479405	MS17-APR: Security update for the libjpeg information disclosure vulnerability in Windows Vista and Windows Server 2008 - Windows Vista SP2 - KB4014794

401498501	MS17-APR: Security Only update for .NET Framework - Security Only - Windows 7 SP1 / Windows Server 2008 R2 SP1 / Windows Vista SP2 / Windows Server 2008 SP2 - .NET Framework 4.5.2 - KB4014566 (x64)
401498503	MS17-APR: Security Only update for .NET Framework - Security Only - Windows 7 SP1 / Windows Vista SP2 / Windows Server 2008 SP2 - .NET Framework 4.5.2 - KB4014566
401498505	MS17-APR: Security Only update for .NET Framework - Security Only - Windows 7 SP1 / Windows Server 2008 R2 SP1 - .NET Framework 4.6.2 - KB4014552 (x64)
401498507	MS17-APR: Security Only update for .NET Framework - Security Only - Windows 7 SP1 - .NET Framework 4.6.2 - KB4014552
401498509	MS17-APR: Security Only update for .NET Framework - Security Only - Windows 7 SP1 / Windows Server 2008 R2 SP1 / Windows Vista SP2 / Windows Server 2008 SP2 - .NET Framework 4.6/4.6.1 - KB4014558 (x64)
401498511	MS17-APR: Security Only update for .NET Framework - Security Only - Windows 7 SP1 / Windows Vista SP2 / Windows Server 2008 SP2 - .NET Framework 4.6/4.6.1 - KB4014558
401498513	MS17-APR: Security Only update for .NET Framework - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4014573 (x64)
401498517	MS17-APR: Security Only update for .NET Framework - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4014573
401498703	MS17-APR: Security Only update for .NET Framework - Security Only - Windows 8.1 - .NET Framework 4.6.2 - KB4014550 (x64)
401498705	MS17-APR: Security Only update for .NET Framework - Security Only - Windows 8.1 - .NET Framework 4.6.2 - KB4014550
401498707	MS17-APR: Security Only update for .NET Framework - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1 - KB4014556 (x64)
401498711	MS17-APR: Security Only update for .NET Framework - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1 - KB4014556
401498713	MS17-APR: Security Only update for .NET Framework - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4014562 (x64)
401498717	MS17-APR: Security Only update for .NET Framework - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4014562
401498721	MS17-APR: Security Only update for .NET Framework - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4014574 (x64)
401498723	MS17-APR: Security Only update for .NET Framework - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4014574
401498813	MS17-APR: Security Only update for .NET Framework - Security Only - Windows Vista SP2 / Windows Server 2008 SP2 - .NET Framework 2.0 SP2 - KB4014571 (x64)
401498815	MS17-APR: Security Only update for .NET Framework - Security Only - Windows Vista SP2 / Windows Server 2008 SP2 - .NET Framework 2.0 SP2 - KB4014571

401506701	MS17-APR: Security update for the scripting engine memory corruption vulnerability in Windows Vista and Windows Server 2008 - Windows Vista SP2 - KB4015067 (x64)
401506707	MS17-APR: Security update for the scripting engine memory corruption vulnerability in Windows Vista and Windows Server 2008 - Windows Vista SP2 - KB4015067
401506801	MS17-APR: Security update for the LDAP elevation of privilege vulnerability in Windows Vista and Windows Server 2008 - Windows Vista SP2 - KB4015068 (x64)
401506805	MS17-APR: Security update for the LDAP elevation of privilege vulnerability in Windows Vista and Windows Server 2008 - Windows Vista SP2 - KB4015068
401519503	MS17-APR: Security update for the Win32k information disclosure vulnerability in Windows Vista and Windows Server 2008 - Windows Vista SP2 - KB4015195 (x64)
401519507	MS17-APR: Security update for the Win32k information disclosure vulnerability in Windows Vista and Windows Server 2008 - Windows Vista SP2 - KB4015195
401538003	MS17-APR: Security update for the ATMFD.Dll information disclosure vulnerability for Windows Vista and Windows Server 2008 - Windows Vista SP2 - KB4015380 (x64)
401538007	MS17-APR: Security update for the ATMFD.Dll information disclosure vulnerability for Windows Vista and Windows Server 2008 - Windows Vista SP2 - KB4015380
401538303	MS17-APR: Security update for the libjpeg information disclosure vulnerability in Windows Vista and Windows Server 2008 - Windows Vista SP2 - KB4015383 (x64)
401538307	MS17-APR: Security update for the libjpeg information disclosure vulnerability in Windows Vista and Windows Server 2008 - Windows Vista SP2 - KB4015383
401554603	MS17-APR: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4015546 (x64)
401554605	MS17-APR: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4015546
401554701	MS17-APR: Security Only Quality Update - Security Only - Windows 8.1 - KB4015547 (x64)
401554705	MS17-APR: Security Only Quality Update - Security Only - Windows 8.1 - KB4015547
401701801	MS17-013: Security update for Microsoft Graphics Component - Windows Vista SP2 - KB4017018 (x64)
401701805	MS17-013: Security update for Microsoft Graphics Component - Windows Vista SP2 - KB4017018
401827119	MS17-JUN: Cumulative security update for Internet Explorer - Windows 7 SP1 - IE 10 - KB4018271

401827121	MS17-JUN: Cumulative security update for Internet Explorer - Windows Vista SP2 - IE 9 - KB4018271 (x64)
401827123	MS17-JUN: Cumulative security update for Internet Explorer - Windows Vista SP2 - IE 9 - KB4018271
401827125	MS17-JUN: Cumulative security update for Internet Explorer - Windows 7 SP1 - IE 9 - KB4018271 (x64)
401827127	MS17-JUN: Cumulative security update for Internet Explorer - Windows 8 - IE 10 - KB4018271 (x64)
401827129	MS17-JUN: Cumulative security update for Internet Explorer - Windows 8 - IE 10 - KB4018271
401827131	MS17-JUN: Cumulative security update for Internet Explorer - Windows 7 SP1 - IE 8 - KB4018271
401827133	MS17-JUN: Cumulative security update for Internet Explorer - Windows 7 SP1 - IE 10 - KB4018271 (x64)
401827135	MS17-JUN: Cumulative security update for Internet Explorer - Windows 7 SP1 - IE 9 - KB4018271
401827137	MS17-JUN: Cumulative security update for Internet Explorer - Windows 7 SP1 - IE 8 - KB4018271 (x64)
401827139	MS17-JUN: Cumulative security update for Internet Explorer - Windows XP - IE 8 - KB4018271 (x64)
401827141	MS17-JUN: Cumulative security update for Internet Explorer - Windows XP - IE 8 - KB4018271
401846605	MS17-JUN: Security update for the Windows SMB Information Disclosure Vulnerability in Windows Server 2008 - Windows Vista SP2 - KB4018466 (x64)
401846607	MS17-JUN: Security update for the Windows SMB Information Disclosure Vulnerability in Windows Server 2008 - Windows Vista SP2 - KB4018466
401846609	MS17-JUN: Security update for the Windows SMB Information Disclosure Vulnerability - Windows Server 2003 SP2 / Windows XP SP2 - KB4018466 (x64)
401846611	MS17-JUN: Security update for the Windows SMB Information Disclosure Vulnerability - Windows XP SP3 - KB4018466
401920405	MS17-JUN: Security update for the Windows win32k Information Disclosure Vulnerability in Windows Server 2008 - Windows Vista SP2 - KB4019204 (x64)
401920407	MS17-JUN: Security update for the Windows win32k Information Disclosure Vulnerability in Windows Server 2008 - Windows Vista SP2 - KB4019204
401920409	MS17-JUN: Security update for the Windows win32k Information Disclosure Vulnerability - Windows Server 2003 SP2 / Windows XP SP2 - KB4019204 (x64)

401920411	MS17-JUN: Security update for the Windows win32k Information Disclosure Vulnerability - Windows XP SP3 - KB4019204
401921303	MS17-MAY: Security Only Quality Update - Security Only - Windows 8.1 - KB4019213 (x64)
401921305	MS17-MAY: Security Only Quality Update - Security Only - Windows 8.1 - KB4019213
401926303	MS17-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4019263 (x64)
401926305	MS17-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4019263
401962301	MS17-JUN: Security Update for Windows 8 - Windows 8 - KB4019623 (x64) (V2.0)
401962303	MS17-JUN: Security Update for Windows 8 - Windows 8 - KB4019623 (V2.0)
401999001	4019990: Update for the d3dcompiler_47.Dll component on Windows Server 2012, Windows 7, and Windows Server 2008 R2 - Windows 7 SP1 - KB4019990 (x64)
401999005	4019990: Update for the d3dcompiler_47.Dll component on Windows Server 2012, Windows 7, and Windows Server 2008 R2 - Windows 7 SP1 - KB4019990
402049901	4020499: Update for the .NET Framework 4.6.2 on Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6.2 - KB4020499 (x64)
402049905	4020499: Update for the .NET Framework 4.6.2 on Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6.2 - KB4020499
402050003	4020500: Update for the .NET Framework 4.6.2 on Windows 7 and Windows Server 2008 R2 - Windows 7 SP1 - .NET Framework 4.6.2 - KB4020500 (x64)
402050005	4020500: Update for the .NET Framework 4.6.2 on Windows 7 and Windows Server 2008 R2 - Windows 7 SP1 - .NET Framework 4.6.2 - KB4020500
402050201	4020502: Update for the .NET Framework 4.6 and 4.6.1 on Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1 - KB4020502 (x64)
402050205	4020502: Update for the .NET Framework 4.6 and 4.6.1 on Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1 - KB4020502
402050301	4020503: Update for the .NET Framework 4.6 and 4.6.1 on Windows 7, Windows Server 2008 R2, and .NET Framework 4.6 on Windows Server 2008 - Windows 7 SP1 - .NET Framework 4.6/4.6.1 - KB4020503 (x64)
402050309	4020503: Update for the .NET Framework 4.6 and 4.6.1 on Windows 7, Windows Server 2008 R2, and .NET Framework 4.6 on Windows Server 2008 - Windows 7 SP1 - .NET Framework 4.6/4.6.1 - KB4020503

402050501	4020505: Update for the .NET Framework 4.5.2 on Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4020505 (x64)
402050505	4020505: Update for the .NET Framework 4.5.2 on Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4020505
402051301	4020513: Update for the .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 - Windows 7 SP1 - .NET Framework 3.5.1 - KB4020513 (x64)
402051305	4020513: Update for the .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 - Windows 7 SP1 - .NET Framework 3.5.1 - KB4020513
402051401	4020514: Update for the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB4020514 (x64)
402051405	4020514: Update for the .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB4020514
402190301	MS17-JUN: LNK remote code execution vulnerability - Windows Vista SP2 - KB4021903 (x64)
402190305	MS17-JUN: LNK remote code execution vulnerability - Windows Vista SP2 - KB4021903
402271703	MS17-JUN: Security Only Quality Update - Security Only - Windows 8.1 - KB4022717 (x64)
402271705	MS17-JUN: Security Only Quality Update - Security Only - Windows 8.1 - KB4022717
402272201	MS17-JUN: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4022722 (x64)
402272205	MS17-JUN: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4022722
402274701	MS17-JUN: Security update of Windows XP and Windows Server 2003 - Windows Server 2003 SP2 / Windows XP SP2 - KB4022747 (x64)
402274703	MS17-JUN: Security update of Windows XP and Windows Server 2003 - Windows Server 2003 SP2 - KB4022747
402274705	MS17-JUN: Security update of Windows XP and Windows Server 2003 - Windows XP SP3 - KB4022747
402283901	MS17-JUN: Security update for Windows 8 - Windows 8 - KB4022839 (x64)
402283903	MS17-JUN: Security update for Windows 8 - Windows 8 - KB4022839
402432301	MS17-JUN: Security update of Windows XP and Windows Server 2003 - Windows Server 2003 SP2 / Windows XP SP2 - KB4024323 (x64)
402432303	MS17-JUN: Security update of Windows XP and Windows Server 2003 - Windows XP SP3 - KB4024323

402432305	MS17-JUN: Security update of Windows XP and Windows Server 2003 - Windows Server 2003 SP2 - KB4024323
402440201	MS17-JUN: Windows search vulnerabilities in Windows Server 2008 - Windows Vista SP2 - KB4024402 (x64)
402440205	MS17-JUN: Windows search vulnerabilities in Windows Server 2008 - Windows Vista SP2 - KB4024402
402440209	MS17-JUN: Windows search vulnerabilities - Windows Server 2003 SP2 / Windows XP SP2 - KB4024402 (x64)
402440211	MS17-JUN: Windows search vulnerabilities - Windows XP SP3 - KB4024402
402521801	MS17-JUN: Security update for Windows XP and Windows Server 2003 - Windows Server 2003 SP2 / Windows XP SP2 - KB4025218 (x64)
402521803	MS17-JUN: Security update for Windows XP and Windows Server 2003 - Windows XP SP3 - KB4025218
402521805	MS17-JUN: Security update for Windows XP and Windows Server 2003 - Windows Server 2003 SP2 - KB4025218
402533303	MS17-JUL: Security Only Quality Update - Security Only - Windows 8.1 - KB4025333 (x64)
402533305	MS17-JUL: Security Only Quality Update - Security Only - Windows 8.1 - KB4025333
402533703	MS17-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4025337 (x64)
402533705	MS17-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4025337
403334217	4033342: UPDATE: Microsoft .NET Framework 4.7.1 Available - Windows 7 SP1 / Windows 8.1 / Windows 2008 R2 SP1 / Windows 2012 / Windows 2012 R2 / Windows 10 / Windows Server 2016
403467203	MS17-AUG: Security Only Quality Update - Security Only - Windows 8.1 - KB4034672 (x64)
403467205	MS17-AUG: Security Only Quality Update - Security Only - Windows 8.1 - KB4034672
403467901	MS17-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4034679 (x64)
403467905	MS17-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4034679
403551003	4035510: Update for the .NET Framework 4.6, 4.6.1, 4.6.2, and 4.7 on Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2 - KB4035510 (x64)
403551005	4035510: Update for the .NET Framework 4.6, 4.6.1, 4.6.2, and 4.7 on Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2 - KB4035510
403877901	MS17-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4038779 (x64)

403877905	MS17-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4038779
403879301	MS17-SEP: Security Only Quality Update - Security Only - Windows 8.1 - KB4038793 (x64)
403879305	MS17-SEP: Security Only Quality Update - Security Only - Windows 8.1 - KB4038793
403892203	4038922: Update for the .NET Framework 4.6, 4.6.1, 4.6.2, and 4.7 on Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7 - KB4038922 (x64)
403892205	4038922: Update for the .NET Framework 4.6, 4.6.1, 4.6.2, and 4.7 on Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7 - KB4038922
404109001	MS17-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4040960 (x64)
404109005	MS17-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4040960
404109009	MS17-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7 - KB4040957 (x64)
404109011	MS17-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7 - KB4040957
404109019	MS17-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4040966 (x64)
404109023	MS17-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4040966
404109203	MS17-SEP: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7 - KB4040956 (x64)
404109205	MS17-SEP: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7 - KB4040956
404109207	MS17-SEP: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4040958 (x64)
404109211	MS17-SEP: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4040958
404109215	MS17-SEP: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4040967 (x64)
404109217	MS17-SEP: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4040967
404167801	MS17-OCT: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4041678 (x64)
404167805	MS17-OCT: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4041678
404168701	MS17-OCT: Security Only Quality Update - Security Only - Windows 8.1 - KB4041687 (x64)

404168705	MS17-OCT: Security Only Quality Update - Security Only - Windows 8.1 - KB4041687
404207619	4042076: Security and Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 3.5.1 - KB4040980 (x64)
404207623	4042076: Security and Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 3.5.1 - KB4040980
404207809	4042078: Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB4040981 (x64)
404207811	4042078: Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB4040981
404376607	4043766: Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, and 4.7 for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7 - KB4043764 (x64)
404376611	4043766: Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, and 4.7 for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7 - KB4043764
404376713	4043767: Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, and 4.7 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7 - KB4043763 (x64)
404376717	4043767: Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, and 4.7 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7 - KB4043763
404896003	MS17-NOV: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4048960
404896005	MS17-NOV: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4048960 (x64)
404896101	MS17-NOV: Security Only Quality Update - Security Only - Windows 8.1 - KB4048961 (x64)
404896105	MS17-NOV: Security Only Quality Update - Security Only - Windows 8.1 - KB4048961
405452101	MS17-DEC: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4054521 (x64)
405452105	MS17-DEC: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4054521
405452201	MS17-DEC: Security Only Quality Update - Security Only - Windows 8.1 - KB4054522 (x64)
405452205	MS17-DEC: Security Only Quality Update - Security Only - Windows 8.1 - KB4054522

405453001	4054530: UPDATE: Microsoft .NET Framework 4.7.2 Available - Windows 7 SP1 / Windows 8.1 / Windows 10 / Windows Server 2008 R2 SP1 / Windows Server 2012 / Windows Server 2012 R2 / Windows Server 2016
405526901	MS18-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4054172 (x64)
405526905	MS18-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4054172
405526907	MS18-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 - KB4054183 (x64)
405526911	MS18-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 - KB4054183
405526921	MS18-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4054176 (x64)
405526923	MS18-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4054176
405527103	MS18-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4054170 (x64)
405527105	MS18-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4054170
405527109	MS18-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 SP1 - KB4054177 (x64)
405527111	MS18-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 SP1 - KB4054177
405527115	MS18-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 - KB4054182 (x64)
405527117	MS18-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 - KB4054182
405689701	MS18-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4056897 (x64)
405689705	MS18-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4056897
405689809	MS18-JAN: Security Only Quality Update - Security Only - Windows 8.1 - KB4056898 (x64) (V2.0)
405689811	MS18-JAN: Security Only Quality Update - Security Only - Windows 8.1 - KB4056898 (V2.0)
407357803	4073578: Unbootable state for AMD devices in Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - KB4073578 (x64)
407357805	4073578: Unbootable state for AMD devices in Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - KB4073578
407458701	MS18-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4074587 (x64)
407458705	MS18-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4074587

407459701	MS18-FEB: Security Only Quality Update - Security Only - Windows 8.1 - KB4074597 (x64)
407459705	MS18-FEB: Security Only Quality Update - Security Only - Windows 8.1 - KB4074597
408887803	MS18-MAR: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4088878 (x64)
408887805	MS18-MAR: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4088878
408887901	MS18-MAR: Security Only Quality Update - Security Only - Windows 8.1 - KB4088879 (x64)
408887905	MS18-MAR: Security Only Quality Update - Security Only - Windows 8.1 - KB4088879
409129003	4091290: Update for Windows 7 - Windows 7 SP1 - KB4091290 (x64)
409129005	4091290: Update for Windows 7 - Windows 7 SP1 - KB4091290
409310803	MS18-APR: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4093108 (x64)
409310805	MS18-APR: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4093108
409311503	MS18-APR: Security Only Quality Update - Security Only - Windows 8.1 - KB4093115 (x64)
409311505	MS18-APR: Security Only Quality Update - Security Only - Windows 8.1 - KB4093115
409551403	MS18-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4095514 (x64)
409551405	MS18-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4095514
409551501	MS18-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 SP1 - KB4095515 (x64)
409551505	MS18-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 SP1 - KB4095515
409551703	MS18-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4095517 (x64)
409551705	MS18-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4095517
409551901	MS18-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4095519 (x64)
409551905	MS18-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4095519
409623601	MS18-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 - KB4096236 (x64)
409623605	MS18-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 - KB4096236

409623701	MS18-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 - KB4096237 (x64)
409623705	MS18-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 - KB4096237
409995001	4099950: Network Interface Card settings can be replaced, or static IP address settings can be lost - Windows 7 SP1 - KB4099950 (x64)
409995005	4099950: Network Interface Card settings can be replaced, or static IP address settings can be lost - Windows 7 SP1 - KB4099950
410371203	MS18-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4103712 (x64)
410371205	MS18-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4103712
410371503	MS18-MAY: Security Only Quality Update - Security Only - Windows 8.1 - KB4103715 (x64)
410371505	MS18-MAY: Security Only Quality Update - Security Only - Windows 8.1 - KB4103715
428486703	MS18-JUN: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4284867 (x64)
428486705	MS18-JUN: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4284867
428487803	MS18-JUN: Security Only Quality Update - Security Only - Windows 8.1 - KB4284878 (x64)
428487805	MS18-JUN: Security Only Quality Update - Security Only - Windows 8.1 - KB4284878
433860001	MS18-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4338600 (x64)
433860005	MS18-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4338600
433860201	MS18-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4338602 (x64)
433860205	MS18-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4338602
433860501	MS18-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 - KB4338605 (x64)
433860505	MS18-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 - KB4338605
433860603	MS18-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 - KB4338606 (x64)
433860605	MS18-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 - KB4338606
433861201	MS18-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4338612 (x64)

433861205	MS18-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4338612
433861303	MS18-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 SP1 - KB4338613 (x64)
433861305	MS18-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 SP1 - KB4338613
433882303	MS18-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4338823 (x64)
433882305	MS18-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4338823
433882401	MS18-JUL: Security Only Quality Update - Security Only - Windows 8.1 - KB4338824 (x64)
433882405	MS18-JUL: Security Only Quality Update - Security Only - Windows 8.1 - KB4338824
434388803	MS18-AUG: Security Only Quality Update - Security Only - Windows 8.1 - KB4343888 (x64)
434388805	MS18-AUG: Security Only Quality Update - Security Only - Windows 8.1 - KB4343888
434389901	MS18-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4343899 (x64)
434389905	MS18-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4343899
434416603	MS18-AUG: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4344166 (x64)
434416605	MS18-AUG: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4344166
434416703	MS18-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4344167 (x64)
434416705	MS18-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4344167
434417101	MS18-AUG: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4344171 (x64)
434417105	MS18-AUG: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4344171
434417307	MS18-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4344173 (x64)
434417309	MS18-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4344173
434417703	MS18-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4344177 (x64)
434417705	MS18-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4344177

434417803	MS18-AUG: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4344178 (x64)
434417805	MS18-AUG: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4344178
434640601	4346406: Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 on Windows 8.1 and Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4346406 (x64)
434640605	4346406: Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 on Windows 8.1 and Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4346406
434640703	4346407: Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 on Windows 7 SP1 and Server 2008 R2 SP1, and .NET Framework 4.6 on Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4346407 (x64)
434640707	4346407: Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 on Windows 7 SP1 and Server 2008 R2 SP1, and .NET Framework 4.6 on Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4346407
434640803	4346408: Update for .NET Framework 4.5.2 on Windows 8.1 and Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4346408 (x64)
434640805	4346408: Update for .NET Framework 4.5.2 on Windows 8.1 and Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4346408
434641001	4346410: Update for .NET Framework 4.5.2 on Windows 7 SP1, Server 2008 R2 SP1, and Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.5.2 - KB4346410 (x64)
434641005	4346410: Update for .NET Framework 4.5.2 on Windows 7 SP1, Server 2008 R2 SP1, and Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.5.2 - KB4346410
434674401	4346744: Update for .NET Framework 3.5.1 on Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 3.5.1 - KB4346744 (x64)
434674405	4346744: Update for .NET Framework 3.5.1 on Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 3.5.1 - KB4346744
434674503	4346745: Update for .NET Framework 3.5 SP1 on Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 SP1 - KB4346745 (x64)
434674505	4346745: Update for .NET Framework 3.5 SP1 on Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 SP1 - KB4346745
445703007	MS18-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4457030 (x64)
445703009	MS18-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4457030

445705503	MS18-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4457055 (x64)
445705505	MS18-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4457055
445705603	MS18-SEP: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4457056 (x64)
445705605	MS18-SEP: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4457056
445714301	MS18-SEP: Security Only Quality Update - Security Only - Windows 8.1 - KB4457143 (x64)
445714305	MS18-SEP: Security Only Quality Update - Security Only - Windows 8.1 - KB4457143
445714503	MS18-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4457145 (x64)
445714505	MS18-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4457145
446290101	4462901: Update for Windows 8.1 - Windows 8.1 - KB4462901 (x64)
446290105	4462901: Update for Windows 8.1 - Windows 8.1 - KB4462901
446291503	MS18-OCT: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4462915 (x64)
446291505	MS18-OCT: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4462915
446294103	MS18-OCT: Security Only Quality Update - Security Only - Windows 8.1 - KB4462941 (x64)
446294105	MS18-OCT: Security Only Quality Update - Security Only - Windows 8.1 - KB4462941
446710603	MS18-NOV: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4467106 (x64)
446710605	MS18-NOV: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4467106
446770301	MS18-NOV: Security Only Quality Update - Security Only - Windows 8.1 - KB4467703 (x64)
446770305	MS18-NOV: Security Only Quality Update - Security Only - Windows 8.1 - KB4467703
446832307	4468323: DST and time zone changes in Windows for Morocco and Volgograd - Windows 7 SP1 - KB4468323 (x64)
446832309	4468323: DST and time zone changes in Windows for Morocco and Volgograd - Windows 7 SP1 - KB4468323
446832313	4468323: DST and time zone changes in Windows for Morocco and Volgograd - Windows 8.1 - KB4468323 (x64)
446832317	4468323: DST and time zone changes in Windows for Morocco and Volgograd - Windows 8.1 - KB4468323

447049101	MS18-DEC: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4470491 (x64)
447049105	MS18-DEC: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4470491
447049301	MS18-DEC: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4470493 (x64)
447049305	MS18-DEC: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4470493
447049901	MS18-DEC: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4470499 (x64)
447049905	MS18-DEC: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4470499
447050001	MS18-DEC: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4470500 (x64)
447050005	MS18-DEC: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4470500
447060001	MS18-DEC: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4470600 (x64)
447060005	MS18-DEC: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4470600
447060201	MS18-DEC: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4470602 (x64)
447060205	MS18-DEC: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4470602
447132203	MS18-DEC: Security Only Quality Update - Security Only - Windows 8.1 - KB4471322 (x64)
447132205	MS18-DEC: Security Only Quality Update - Security Only - Windows 8.1 - KB4471322
447132803	MS18-DEC: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4471328 (x64)
447132805	MS18-DEC: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4471328
447441925	MS19-SEP: SHA-2 code signing support update for Windows Server 2008 R2, Windows 7, and Windows Server 2008 - Windows 7 SP1 - KB4474419 (x64) (V3.0)
447441929	MS19-SEP: SHA-2 code signing support update for Windows Server 2008 R2, Windows 7, and Windows Server 2008 - Windows 7 SP1 - KB4474419 (V3.0)
448007101	MS19-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4480071 (x64)
448007105	MS19-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4480071

448007203	MS19-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4480072 (x64)
448007207	MS19-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4480072
448007403	MS19-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4480074 (x64)
448007405	MS19-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4480074
448007601	MS19-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4480076 (x64)
448007609	MS19-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4480076
448008501	MS19-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4480085 (x64)
448008505	MS19-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4480085
448008603	MS19-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4480086 (x64)
448008605	MS19-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4480086
448096003	MS19-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4480960 (x64)
448096005	MS19-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4480960
448096403	MS19-JAN: Security Only Quality Update - Security Only - Windows 8.1 - KB4480964 (x64)
448096405	MS19-JAN: Security Only Quality Update - Security Only - Windows 8.1 - KB4480964
448345003	MS19-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4483450 (x64)
448345005	MS19-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4483450
448345109	MS19-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4483451
448345301	MS19-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.5.2 - KB4483453 (x64)
448345305	MS19-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.5.2 - KB4483453
448345903	MS19-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 3.5 - KB4483459 (x64)
448345905	MS19-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 3.5 - KB4483459

448346901	MS19-FEB: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4483469 (x64)
448346905	MS19-FEB: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4483469
448347005	MS19-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4483470 (x64)
448347009	MS19-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4483470
448347203	MS19-FEB: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4483472 (x64)
448347205	MS19-FEB: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4483472
448347405	MS19-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4483474 (x64)
448347409	MS19-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4483474
448348303	MS19-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4483483 (x64)
448348305	MS19-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4483483
448348403	MS19-FEB: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4483484 (x64)
448348405	MS19-FEB: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4483484
448610501	4486105: Microsoft .NET Framework 4.8 for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4486105 (x64)
448610505	4486105: Microsoft .NET Framework 4.8 for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4486105
448645907	4486459: DST changes in Windows for Chile - Windows 7 SP1 - KB4486459 (x64)
448645909	4486459: DST changes in Windows for Chile - Windows 7 SP1 - KB4486459
448645911	4486459: DST changes in Windows for Chile - Windows 8.1 - KB4486459 (x64)
448645915	4486459: DST changes in Windows for Chile - Windows 8.1 - KB4486459
448656403	MS19-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4486564 (x64)
448656405	MS19-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4486564
448702803	MS19-FEB: Security Only Quality Update - Security Only - Windows 8.1 - KB4487028 (x64)

448702805	MS19-FEB: Security Only Quality Update - Security Only - Windows 8.1 - KB4487028
448712303	4487123: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 and Server 2012 R2 for x64 - Windows 8.1 - .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 - KB4483469 (x64)
448712305	4487123: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 - Windows 8.1 - .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 - KB4483469
448712309	4487123: Security Only Update for .NET Framework 4.5.2 for Windows 8.1 and Server 2012 R2 for x64 - Windows 8.1 - .NET Framework 4.5.2 - KB4483472 (x64)
448712311	4487123: Security Only Update for .NET Framework 4.5.2 for Windows 8.1 - Windows 8.1 - .NET Framework 4.5.2 - KB4483472
448712313	4487123: Security Only Update for .NET Framework 3.5 for Windows 8.1 and Server 2012 R2 for x64 - Windows 8.1 - .NET Framework 3.5 - KB4483484 (x64)
448712317	4487123: Security Only Update for .NET Framework 3.5 for Windows 8.1 - Windows 8.1 - .NET Framework 3.5 - KB4483484
448948609	4489486: Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 for Windows 7 SP1 and Server 2008 R2 SP1 and 4.6 for Windows Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4488666 (x64)
448948611	4489486: Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 for Windows 7 SP1 and Server 2008 R2 SP1 and 4.6 for Windows Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4488666
448948613	4489486: Update for .NET Framework 4.5.2 for Windows 7 SP1, Server 2008 R2 SP1 and Windows Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.5.2 - KB4488669 (x64) (V2.0)
448948617	4489486: Update for .NET Framework 4.5.2 for Windows 7 SP1, Server 2008 R2 SP1 and Windows Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.5.2 - KB4488669 (V2.0)
448948621	4489486: Update for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 3.5.1 - KB4488662 (x64)
448948623	4489486: Update for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 3.5.1 - KB4488662
448948801	4489488: Update for .NET Framework 3.5 for Windows 8.1 and Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB4488663 (x64)
448948805	4489488: Update for .NET Framework 3.5 for Windows 8.1 and Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB4488663

448948809	4489488: Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 for Windows 8.1 and Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4488665 (x64)
448948811	4489488: Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, and 4.7.2 for Windows 8.1 and Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4488665
448948815	4489488: Update for .NET Framework 4.5.2 for Windows 8.1 and Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4488667 (x64)
448948817	4489488: Update for .NET Framework 4.5.2 for Windows 8.1 and Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4488667
448988303	MS19-MAR: Security Only Quality Update - Security Only - Windows 8.1 - KB4489883 (x64)
448988305	MS19-MAR: Security Only Quality Update - Security Only - Windows 8.1 - KB4489883
448988501	MS19-MAR: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4489885 (x64)
448988505	MS19-MAR: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4489885
449012807	4490128: Time zone changes in Windows for Sao Tome and Principe, and Qyzylorda - Windows 7 SP1 - KB4490128 (x64)
449012809	4490128: Time zone changes in Windows for Sao Tome and Principe, and Qyzylorda - Windows 7 SP1 - KB4490128
449012815	4490128: Time zone changes in Windows for Sao Tome and Principe, and Qyzylorda - Windows 8.1 - KB4490128 (x64)
449012817	4490128: Time zone changes in Windows for Sao Tome and Principe, and Qyzylorda - Windows 8.1 - KB4490128
449062803	MS19-MAR: Servicing stack update for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - KB4490628 (x64)
449062805	MS19-MAR: Servicing stack update for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - KB4490628
449287201	4492872: Internet Explorer 11 Available - Prerequisites - Windows Server 2012 (x64)
449287203	4492872: Internet Explorer 11 Available - Install - Windows Server 2012 (x64)
449344803	MS19-APR: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4493448 (x64)
449344805	MS19-APR: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4493448
449346703	MS19-APR: Security Only Quality Update - Security Only - Windows 8.1 - KB4493467 (x64)
449346705	MS19-APR: Security Only Quality Update - Security Only - Windows 8.1 - KB4493467

449558501	MS19-MAY: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4495585 (x64)
449558505	MS19-MAY: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4495585
449558601	MS19-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4495586 (x64)
449558605	MS19-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4495586
449558701	MS19-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4495587 (x64)
449558705	MS19-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4495587
449558901	MS19-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4495589 (x64)
449558905	MS19-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4495589
449559303	MS19-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4495593 (x64)
449559305	MS19-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4495593
449561201	MS19-MAY: Security Only Update for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 and Server 2008 - Windows 7 SP1 - .NET Framework 3.5.1 - KB4495612 (x64)
449561205	MS19-MAY: Security Only Update for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 and Server 2008 - Windows 7 SP1 - .NET Framework 3.5.1 - KB4495612
449561503	MS19-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4495615 (x64)
449561505	MS19-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4495615
449562403	MS19-MAY: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.8 - KB4495624 (x64)
449562405	MS19-MAY: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.8 - KB4495624
449562501	MS19-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB4495625 (x64)
449562505	MS19-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB4495625
449562701	MS19-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.8 - KB4495627 (x64)
449562705	MS19-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.8 - KB4495627

449916501	MS19-MAY: Security Only Quality Update - Security Only - Windows 8.1 - KB4499165 (x64)
449916505	MS19-MAY: Security Only Quality Update - Security Only - Windows 8.1 - KB4499165
449917501	MS19-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4499175 (x64)
449917505	MS19-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4499175
449918005	MS19-MAY: Security Only Quality Update - Security Only - Windows Vista SP2 - KB4499180
449918007	MS19-MAY: Security Only Quality Update - Security Only - Windows Vista SP2 - KB4499180 (x64)
450033101	MS19-MAY: Security update for the remote code execution vulnerability - Windows Server 2003 SP2 / Windows XP SP2 - KB4500331 (x64)
450033105	MS19-MAY: Security update for the remote code execution vulnerability - Windows XP SP3 - KB4500331
450122607	4501226: DST changes in Windows for Morocco and the Palestinian Authority - Windows 7 SP1 - KB4501226 (x64)
450122609	4501226: DST changes in Windows for Morocco and the Palestinian Authority - Windows 7 SP1 - KB4501226
450122615	4501226: DST changes in Windows for Morocco and the Palestinian Authority - Windows 8.1 - KB4501226 (x64)
450122617	4501226: DST changes in Windows for Morocco and the Palestinian Authority - Windows 8.1 - KB4501226
450326903	MS19-JUN: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4503269 (x64)
450326905	MS19-JUN: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4503269
450329001	MS19-JUN: Security Only Quality Update - Security Only - Windows 8.1 - KB4503290 (x64)
450329005	MS19-JUN: Security Only Quality Update - Security Only - Windows 8.1 - KB4503290
450695501	MS19-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB4506955 (x64)
450695505	MS19-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB4506955
450695603	MS19-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.8 - KB4506956 (x64)
450695605	MS19-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.8 - KB4506956
450696201	MS19-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4506962 (x64)

450696205	MS19-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4506962
450696303	MS19-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4506963 (x64)
450696305	MS19-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4506963
450696401	MS19-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4506964 (x64)
450696405	MS19-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4506964
450696601	MS19-JUL: Security Only Update for .NET Framework 4.5.2 for Windows 7 SP1 and Server 2008 R2 SP1 and Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.5.2 - KB4506966 (x64)
450696609	MS19-JUL: Security Only Update for .NET Framework 4.5.2 for Windows 7 SP1 and Server 2008 R2 SP1 and Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.5.2 - KB4506966
450697601	MS19-JUL: Security Only Update for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 3.5.1 - KB4506976 (x64)
450697605	MS19-JUL: Security Only Update for .NET Framework 3.5.1 for Windows 7 SP1 and Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 3.5.1 - KB4506976
450697701	MS19-JUL: Security Only Update for .NET Framework 3.5 for Windows 8.1 and Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB4506977 (x64)
450697705	MS19-JUL: Security Only Update for .NET Framework 3.5 for Windows 8.1 and Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB4506977
450699301	MS19-JUL: Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4506993 (x64)
450699305	MS19-JUL: Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4506993
450699603	MS19-JUL: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4506996 (x64)
450699605	MS19-JUL: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4506996
450745603	MS19-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4507456 (x64)

450745605	MS19-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4507456
450745703	MS19-JUL: Security Only Quality Update - Security Only - Windows 8.1 - KB4507457 (x64)
450745705	MS19-JUL: Security Only Quality Update - Security Only - Windows 8.1 - KB4507457
450770405	4507704: DST changes in Windows for Brazil and Morocco - Windows 7 SP1 - KB4507704 (x64)
450770409	4507704: DST changes in Windows for Brazil and Morocco - Windows 7 SP1 - KB4507704
450770415	4507704: DST changes in Windows for Brazil and Morocco - Windows 8.1 - KB4507704 (x64)
450770417	4507704: DST changes in Windows for Brazil and Morocco - Windows 8.1 - KB4507704
450877201	4508772: Update for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - KB4508772 (x64)
450877205	4508772: Update for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - KB4508772
450877303	4508773: Update for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - KB4508773 (x64)
450877305	4508773: Update for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - KB4508773
451248603	MS19-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4512486 (x64)
451248605	MS19-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4512486
451248903	MS19-AUG: Security Only Quality Update - Security Only - Windows 8.1 - KB4512489 (x64)
451248905	MS19-AUG: Security Only Quality Update - Security Only - Windows 8.1 - KB4512489
451433103	MS19-SEP: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB4514331 (x64)
451433105	MS19-SEP: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB4514331
451433801	MS19-SEP: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4514338 (x64)
451433805	MS19-SEP: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4514338
451434103	MS19-SEP: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4514341 (x64)
451434105	MS19-SEP: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4514341

451435003	MS19-SEP: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4514350 (x64)
451435005	MS19-SEP: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4514350
451603303	MS19-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4516033 (x64)
451603305	MS19-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4516033
451606401	MS19-SEP: Security Only Quality Update - Security Only - Windows 8.1 - KB4516064 (x64)
451606405	MS19-SEP: Security Only Quality Update - Security Only - Windows 8.1 - KB4516064
451655315	4516553: Preview of Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4515846 (x64)
451655317	4516553: Preview of Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4515846
451655321	4516553: Preview of Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4515853 (x64)
451655323	4516553: Preview of Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4515853
451910805	4519108: DST changes in Windows for Norfolk Island and Fiji Island - Windows 7 SP1 - KB4519108 (x64)
451910809	4519108: DST changes in Windows for Norfolk Island and Fiji Island - Windows 7 SP1 - KB4519108
451910813	4519108: DST changes in Windows for Norfolk Island and Fiji Island - Windows 8.1 - KB4519108 (x64)
451910817	4519108: DST changes in Windows for Norfolk Island and Fiji Island - Windows 8.1 - KB4519108
451956701	4519567: Preview of Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4519567 (x64)
451956705	4519567: Preview of Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4519567
451957103	4519571: Preview of Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4519571 (x64)
451957105	4519571: Preview of Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4519571

451999001	MS19-NOV / MS19-OCT: Security Only Quality Update - Security Only - Windows 8.1 - KB4519990 (x64)
451999005	MS19-NOV / MS19-OCT: Security Only Quality Update - Security Only - Windows 8.1 - KB4519990
452000301	MS19-NOV / MS19-OCT: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4520003 (x64)
452000305	MS19-NOV / MS19-OCT: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4520003
452523301	MS19-NOV: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4525233
452523305	MS19-NOV: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4525233 (x64)
452525003	MS19-NOV: Security Only Quality Update - Security Only - Windows 8.1 - KB4525250 (x64)
452525005	MS19-NOV: Security Only Quality Update - Security Only - Windows 8.1 - KB4525250
453069203	MS19-DEC: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4530692 (x64)
453069205	MS19-DEC: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4530692
453073001	MS19-DEC: Security Only Quality Update - Security Only - Windows 8.1 - KB4530730 (x64)
453073005	MS19-DEC: Security Only Quality Update - Security Only - Windows 8.1 - KB4530730
453074501	4530745: Update for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4530745 (x64)
453074505	4530745: Update for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4530745
453074601	4530746: Update for .NET Framework 4.8 for Windows 7 SP1 and Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 4.8 - KB4530746 (x64)
453074605	4530746: Update for .NET Framework 4.8 for Windows 7 SP1 and Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 4.8 - KB4530746
453118103	4531181: Preview of Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4531181 (x64)
453118105	4531181: Preview of Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4531181
453292905	MS20-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 - .NET Framework 4.5.2 - KB4532929 (x64)
453292909	MS20-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 - .NET Framework 4.5.2 - KB4532929

453293205	MS20-JAN: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 SP1 and Windows Server 2008 R2 SP1 and Windows Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4532932 (x64)
453293207	MS20-JAN: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 SP1 and Windows Server 2008 R2 SP1 and Windows Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4532932
453294003	MS20-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.8 - KB4532940 (x64)
453294005	MS20-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.8 - KB4532940
453294103	MS20-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 - .NET Framework 4.8 - KB4532941 (x64)
453294105	MS20-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 - .NET Framework 4.8 - KB4532941
453294501	MS20-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 - .NET Framework 3.5.1 - KB4532945 (x64)
453294505	MS20-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 - .NET Framework 3.5.1 - KB4532945
453294601	MS20-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 3.5 - KB4532946 (x64)
453294605	MS20-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 3.5 - KB4532946
453295101	MS20-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB4532951 (x64)
453295105	MS20-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB4532951
453295203	MS20-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.8 - KB4532952 (x64)
453295205	MS20-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.8 - KB4532952
453296003	MS20-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4532960 (x64)
453296005	MS20-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 3.5.1 - KB4532960
453296103	MS20-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4532961 (x64)
453296105	MS20-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4532961
453296203	MS20-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4532962 (x64)

453296205	MS20-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4532962
453296403	MS20-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4532964 (x64)
453296405	MS20-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - .NET Framework 4.5.2 - KB4532964
453297001	MS20-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4532970 (x64)
453297005	MS20-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4532970
453297105	MS20-JAN: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4532971 (x64)
453297109	MS20-JAN: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4532971
453412001	4534120: Preview of Quality Rollup for .NET Framework 4.5.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4534120 (x64)
453412005	4534120: Preview of Quality Rollup for .NET Framework 4.5.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4534120
453413403	4534134: Preview of Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4534134 (x64)
453413405	4534134: Preview of Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4534134
453425101	MS20-JAN: Cumulative security update for Internet Explorer - Windows 7 SP1 - IE 11 - KB4534251 (x64)
453425103	MS20-JAN: Cumulative security update for Internet Explorer - Windows Server 2008 R2 SP1 - IE 11 - KB4534251 (x64)
453425105	MS20-JAN: Cumulative security update for Internet Explorer - Windows 7 SP1 - IE 11 - KB4534251
453430903	MS20-JAN: Security Only Quality Update - Security Only - Windows 8.1 - KB4534309 (x64)
453430905	MS20-JAN: Security Only Quality Update - Security Only - Windows 8.1 - KB4534309
453431003	MS20-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 - KB4534310 (x64)
453431005	MS20-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 - KB4534310

453431401	MS20-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4534314 (x64)
453431405	MS20-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 - KB4534314
453567401	4535674: Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB4532946 (x64)
453567405	4535674: Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB4532946
453567409	4535674: Preview of Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4534117 (x64)
453567411	4535674: Preview of Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4534117
453567413	4535674: Preview of Quality Rollup for .NET Framework 4.5.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4534120 (x64)
453567417	4535674: Preview of Quality Rollup for .NET Framework 4.5.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4534120
453567419	4535674: Preview of Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4534134 (x64)
453567423	4535674: Preview of Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4534134
453695203	MS20-JAN: Servicing stack update for Windows 7 SP1 and Server 2008 R2 SP1 - Windows 7 SP1 - KB4536952 (x64)
453695205	MS20-JAN: Servicing stack update for Windows 7 SP1 and Server 2008 R2 SP1 - Windows 7 SP1 - KB4536952
453748201	4537482: Preview of Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4537482 (x64)
453748205	4537482: Preview of Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4537482
453780303	MS20-FEB: Security Only Quality Update - Security Only - Windows 8.1 - KB4537803 (x64)
453780305	MS20-FEB: Security Only Quality Update - Security Only - Windows 8.1 - KB4537803

453781301	MS20-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4537813 (x64)
453781305	MS20-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded)- KB4537813
453781901	4537819: KB4537819 (Preview of Monthly Rollup) - Windows 8.1 - KB4537819 (x64)
453815803	4538158: Preview of Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4537488 (x64)
453815805	4538158: Preview of Quality Rollup for .NET Framework 4.5.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4537491
453815813	4538158: Preview of Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4537488
453815817	4538158: Preview of Quality Rollup for .NET Framework 4.5.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4537491 (x64)
453815819	4538158: Preview of Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB4537503 (x64)
453815823	4538158: Preview of Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB4537503
454150001	MS20-MAR: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4541500
454150003	MS20-MAR: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4541500 (x64)
454150501	MS20-MAR: Security Only Quality Update - Security Only - Windows 8.1 - KB4541505 (x64)
454150505	MS20-MAR: Security Only Quality Update - Security Only - Windows 8.1 - KB4541505
455096501	MS20-APR: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4550965 (x64)
455096505	MS20-APR: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4550965
455097001	MS20-APR: Security Only Quality Update - Security Only - Windows 8.1 - KB4550970 (x64)
455097005	MS20-APR: Security Only Quality Update - Security Only - Windows 8.1 - KB4550970

455291902	MS20-MAY: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 (Embedded) - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4552919 (x64)
455291906	MS20-MAY: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 (Embedded) - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4552919
455294001	MS20-MAY: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 (Embedded) - .NET Framework 3.5.1 - KB4552940 (x64)
455294005	MS20-MAY: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1(Embedded) - .NET Framework 3.5.1 - KB4552940
455295101	MS20-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4552951
455295107	MS20-MAY: Security Only Quality Update - Security Only - Windows 7 SP1(Embedded) - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4552951 (x64)
455295205	MS20-MAY: Security Only Quality Update - Security Only - Windows 7 SP1(Embedded) - .NET Framework 4.5.2 - KB4552952 (x64)
455295207	MS20-MAY: Security Only Quality Update - Security Only - Windows 7 SP1(Embedded) - .NET Framework 4.5.2 - KB4552952
455295301	MS20-MAY: Security Only Quality Update - Security Only - Windows 7 SP1(Embedded) - .NET Framework 4.8 - KB4552953 (x64)
455295303	MS20-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 4.8 - KB4552953
455295908	MS20-MAY: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4552959 (x64)
455295909	MS20-MAY: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4552959
455296206	MS20-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB4552962 (x64)
455296209	MS20-MAY: Security Only Update for .NET Framework 4.8 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4552962
455296501	MS20-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 3.5.1 - KB4552965 (x64)
455296503	MS20-MAY: Security Only Quality Update - Security Only - Windows 7 SP1(Embedded) - .NET Framework 3.5.1 - KB4552965
455296606	MS20-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4552966 (x64)

455296609	MS20-MAY: Security Only Update for .NET Framework 3.5 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB4552966
455296703	MS20-MAY: Security Only Update for .NET Framework 4.5.2 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4552967
455296706	MS20-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4552967 (x64)
455640114	MS20-MAY: Security and Quality Rollup for .NET Framework 4.5.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4552946 (x64)
455640118	MS20-MAY: Security and Quality Rollup for .NET Framework 4.5.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4552946
455640119	MS20-MAY: Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB4552982 (x64)
455640124	MS20-MAY: Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB4552982
455679807	MS20-MAY: Cumulative security update for Internet Explorer - Windows 7 SP1(Embedded) - IE 11 - KB4556798 (x64)
455679811	MS20-MAY: Cumulative security update for Internet Explorer - Windows 7 SP1 (Embedded) - IE 11 - KB4556798
455684301	MS20-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4556843
455684303	MS20-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4556843 (x64)
455685303	MS20-MAY: Security Only Quality Update - Security Only - Windows 8.1 - KB4556853 (x64)
455685305	MS20-MAY: Security Only Quality Update - Security Only - Windows 8.1 - KB4556853
455790015	4557900: DST changes in Windows for Morocco - Windows 8.1 - KB4557900 (x64)
455790017	4557900: DST changes in Windows for Morocco - Windows 8.1 - KB4557900
456166901	MS20-JUN: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4561669 (x64)
456166905	MS20-JUN: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4561669
456167301	MS20-JUN: Security Only Quality Update - Security Only - Windows 8.1 - KB4561673 (x64)

456167305	MS20-JUN: Security Only Quality Update - Security Only - Windows 8.1 - KB4561673
456553903	MS20-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded)- KB4565539 (x64)
456553905	MS20-JUL: Security Only Quality Update - Security Only - Windows 7 SP1(Embedded) - KB4565539
456554001	MS20-JUL: Security Only Quality Update - Security Only - Windows 8.1 - KB4565540 (x64)
456554005	MS20-JUL: Security Only Quality Update - Security Only - Windows 8.1 - KB4565540
456557901	MS20-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 3.5.1 - KB4565579 (x64) (V2.0)
456557905	MS20-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 3.5.1 - KB4565579 (V2.0)
456557909	4565579: Security Only Update for .NET Framework 3.5.1 for Windows 7 SP1 - Windows 7 SP1 (Embedded)- .NET Framework 3.5.1 - KB4565579 (V3.0)
456557915	4565579: Security Only Update for .NET Framework 3.5.1 for Windows 7 SP1- Windows 7 SP1 (Embedded) - .NET Framework 3.5.1 - KB4565579 (x64) (V3.0)
456558001	MS20-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4565580 (x64) (V2.0)
456558005	MS20-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4565580 (V2.0)
456558009	4565580: Security Only Update for .NET Framework 3.5 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB4565580 (x64) (V3.0)
456558011	4565580: Security Only Update for .NET Framework 3.5 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB4565580 (V3.0)
456558101	MS20-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4565581 (x64)
456558105	MS20-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4565581
456558109	4565581: Security Only Update for .NET Framework 4.5.2 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4565581 (x64) (V2.0)
456558111	4565581: Security Only Update for .NET Framework 4.5.2 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4565581 (V2.0)
456558307	MS20-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 4.5.2 - KB4565583 (x64)

456558309	MS20-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded)- .NET Framework 4.5.2 - KB4565583
456558313	4565583: Security Only Update for .NET Framework 4.5.2 for Windows 7 SP1 - Windows 7 SP1(Embedded) - .NET Framework 4.5.2 - KB4565583 (V3.0)
456558315	4565583: Security Only Update for .NET Framework 4.5.2 for Windows 7 SP1 - Windows 7 SP1 (Embedded)- .NET Framework 4.5.2 - KB4565583 (x64) (V3.0)
456558501	MS20-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4565585 (x64)
456558505	MS20-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4565585
456558509	4565585: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4565585 (x64)
456558511	4565585: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4565585
456558605	MS20-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4565586 (x64)
456558609	MS20-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4565586
456558613	4565586: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 SP1 - Windows 7 SP1 (Embedded)- .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4565586 (V3.0)
456558615	4565586: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 SP1 - Windows 7 SP1 (Embedded) - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4565586 (x64) (V3.0)
456558803	MS20-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB4565588 (x64)
456558805	MS20-JUL: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB4565588
456558809	4565588: Security Only Update for .NET Framework 4.8 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4565588 (x64)
456558811	4565588: Security Only Update for .NET Framework 4.8 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4565588
456558903	MS20-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 4.8 - KB4565589 (x64)
456558905	MS20-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded)- .NET Framework 4.8 - KB4565589

456558907	4565589: Security Only Update for .NET Framework 4.8 for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 (Embedded)- .NET Framework 4.8 - KB4565589 (x64) (V3.0)
456558909	4565589: Security Only Update for .NET Framework 4.8 for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 (Embedded)- .NET Framework 4.8 - KB4565589 (V3.0)
456561201	MS20-JUL: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 (Embedded) - .NET Framework 3.5.1 - KB4565612 (x64) (V2.0)
456561203	MS20-JUL: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 (Embedded)- .NET Framework 3.5.1 - KB4565612 (V2.0)
456561607	MS20-JUL: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 (Embedded) - .NET Framework 4.5.2 - KB4565616 (x64)
456561609	MS20-JUL: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 (Embedded)- .NET Framework 4.5.2 - KB4565616
456562305	MS20-JUL: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 SP1 and Windows Server 2008 R2 SP1 and Windows Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4565623 (x64)
456562309	MS20-JUL: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 SP1 and Windows Server 2008 R2 SP1 and Windows Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4565623
456563601	MS20-JUL: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 (Embedded) - .NET Framework 4.8 - KB4565636 (x64)
456563605	MS20-JUL: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 (Embedded)- .NET Framework 4.8 - KB4565636
456637111	4566371: DST changes in Windows for Yukon, Canada - Windows 8.1 - KB4566371 (x64)
456637115	4566371: DST changes in Windows for Yukon, Canada - Windows 8.1 - KB4566371
456973201	MS20-AUG: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB4569732 (x64)
456973205	MS20-AUG: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB4569732
456973601	MS20-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded)- .NET Framework 3.5.1 - KB4569736 (x64)
456973605	MS20-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded)- .NET Framework 3.5.1 - KB4569736
456973703	MS20-AUG: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4569737 (x64)
456973705	MS20-AUG: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4569737

456973903	MS20-AUG: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4569739 (x64)
456973905	MS20-AUG: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4569739
456974001	MS20-AUG: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 SP1 and Windows Server 2008 R2 SP1 and Windows Server 2008 SP2 - Windows 7 SP1 (Embedded)- .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4569740 (x64
456974009	MS20-AUG: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 - Windows 7 SP1 (Embedded)- .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4569740
456974101	MS20-AUG: Security Only Update for .NET Framework 4.5.2 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4569741 (x64)
456974105	MS20-AUG: Security Only Update for .NET Framework 4.5.2 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.5.2 - KB4569741
456974307	MS20-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 4.5.2 - KB4569743 (x64)
456974309	MS20-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded)- .NET Framework 4.5.2 - KB4569743
457050601	MS20-AUG: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 / Windows Server 2008 R2 SP1 - .NET Framework 3.5.1(Embedded) - KB4570506 (x64)
457171903	MS20-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded)- KB4571719 (x64)
457648901	MS20-SEP: Security Only Update for .NET Framework 4.8 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4576489 (x64)
457648905	MS20-SEP: Security Only Update for .NET Framework 4.8 for Windows 8.1 and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4576489
457649001	MS20-SEP: Security Only Update for .NET Framework 4.8 for Windows 7 SP1 - Windows 7 SP1 (Embedded)- .NET Framework 4.8 - KB4576490 (x64)
457649005	MS20-SEP: Security Only Update for .NET Framework 4.8 for Windows 7 SP1 - Windows 7 SP1 (Embedded)- .NET Framework 4.8 - KB4576490
457662807	4576628: Security and Quality Rollup for .NET Framework 4.5.2 for Windows 7 SP1 and Windows Server 2008 R2 SP1 and Windows Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.5.2 - KB4569780 (x64)

457662809	4576628: Security and Quality Rollup for .NET Framework 4.5.2 for Windows 7 SP1 and Windows Server 2008 R2 SP1 and Windows Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.5.2 - KB4569780
457662811	4576628: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 SP1 and Windows Server 2008 R2 SP1 and Windows Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4576612 (x64)
457662815	4576628: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 SP1 and Windows Server 2008 R2 SP1 and Windows Server 2008 SP2 - Windows 7 SP1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4576612
457662817	4576628: Security and Quality Rollup for .NET Framework 4.8 for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 4.8 - KB4576487 (x64)
457662821	4576628: Security and Quality Rollup for .NET Framework 4.8 for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 4.8 - KB4576487
457662829	4576628: Security and Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 3.5.1 - KB4569767 (x64)
457662833	4576628: Security and Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 - .NET Framework 3.5.1 - KB4569767
457705303	MS20-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4577053 (x64)
457705305	MS20-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4577053
457707103	MS20-SEP: Security Only Quality Update - Security Only - Windows 8.1 - KB4577071 (x64)
457707105	MS20-SEP: Security Only Quality Update - Security Only - Windows 8.1 - KB4577071
457758649	4577586: Update for the removal of Adobe Flash Player - Windows 8.1 - Adobe Flash Player - KB4577586 (x64)
457758651	4577586: Update for the removal of Adobe Flash Player - Windows 8.1 - Adobe Flash Player - KB4577586
457862313	4578623: DST correction in Windows for the Fiji Islands - Windows 8.1 - KB4578623 (x64)
457862317	4578623: DST correction in Windows for the Fiji Islands - Windows 8.1 - KB4578623
457895203	MS20-OCT: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 (Embedded) - .NET Framework 3.5.1 - KB4578952 (x64)
457895205	MS20-OCT: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1(Embedded) - .NET Framework 3.5.1 - KB4578952

457896203	MS20-OCT: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4578962 (x64)
457896205	MS20-OCT: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4578962
457896303	MS20-OCT: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 (Embedded) - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4578963 (x64)
457896307	MS20-OCT: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 - Windows 7 SP1(Embedded) - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4578963
457897603	MS20-OCT: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.8 - KB4578976 (x64)
457897605	MS20-OCT: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.8 - KB4578976
457898003	MS20-OCT: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 3.5.1 - KB4578980 (x64)
457898005	MS20-OCT: Security Only Quality Update - Security Only - Windows 7 SP1(Embedded) - .NET Framework 3.5.1 - KB4578980
457898101	MS20-OCT: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4578981 (x64)
457898109	MS20-OCT: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB4578981
457898301	MS20-OCT: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 4.5.2 - KB4578983 (x64)
457898305	MS20-OCT: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 4.5.2 - KB4578983
457898403	MS20-OCT: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB4578984 (x64)
457898409	MS20-OCT: Security Only Update - Windows 8.1 - .NET Framework 4.5.2 - KB4578984
457898601	MS20-OCT: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4578986 (x64)
457898605	MS20-OCT: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4578986
457898701	MS20-OCT: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4578987 (x64)
457898707	MS20-OCT: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 - Windows 7 SP1 (Embedded) - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4578987

457898901	MS20-OCT: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB4578989 (x64)
457898909	MS20-OCT: Security Only Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB4578989
457899003	MS20-OCT: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 4.8 - KB4578990 (x64)
457899005	MS20-OCT: Security Only Quality Update - Security Only - Windows 7 SP1(Embedded) - .NET Framework 4.8 - KB4578990
457997745	MS21-MAR: Security and Quality Rollup - Windows 7 SP1 (Embedded) - .NET Framework 4.5.2 - KB4578955 (V2.0)
457997747	MS21-MAR: Security and Quality Rollup - Windows 7 SP1 (Embedded) - .NET Framework 4.5.2 - KB4578955 (x64) (V2.0)
458032543	MS20-OCT: Security Update for Adobe Flash Player - Windows 8.1 - Adobe Flash Player - KB4580325 (x64)
458032547	MS20-OCT: Security Update for Adobe Flash Player - Windows 8.1 - Adobe Flash Player - KB4580325
458035803	MS20-OCT: Security Only Quality Update - Security Only - Windows 8.1 - KB4580358 (x64)
458035805	MS20-OCT: Security Only Quality Update - Security Only - Windows 8.1 - KB4580358
458038701	MS20-OCT: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4580387 (x64)
458038705	MS20-OCT: Security Only Quality Update - Security Only - Windows 7 SP1(Embedded) - KB4580387
458520401	4586083: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 SP1 - Windows 7 SP1 (Embedded) - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4585204 (x64)
458520415	4586083: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 SP1 - Windows 7 SP1 (Embedded) - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4585204
458520501	4586083: Security and Quality Rollup for .NET Framework 4.8 for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 (Embeeded) - .NET Framework 4.8 - KB4585205 (x64)
458520505	4586083: Security and Quality Rollup for .NET Framework 4.8 for Windows 7 SP1 and Windows Server 2008 R2 SP1 - Windows 7 SP1 (Embedded) - .NET Framework 4.8 - KB4585205
458521201	4586085: Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4585212 (x64)
458521205	4586085: Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB4585212

458521403	4586085: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4585214 (x64)
458521405	4586085: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4585214
458680503	MS20-NOV: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4586805 (x64)
458680505	MS20-NOV: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4586805
458682303	MS20-NOV: Security Only Quality Update - Security Only - Windows 8.1 - KB4586823
458682305	MS20-NOV: Security Only Quality Update - Security Only - Windows 8.1 - KB4586823 (x64)
459249503	MS20-DEC: Security Only Quality Update - Security Only - Windows 8.1 - KB4592495 (x64)
459249505	MS20-DEC: Security Only Quality Update - Security Only - Windows 8.1 - KB4592495
459250301	MS20-DEC: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4592503 (x64)
459250305	MS20-DEC: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4592503
459443901	4594439: Kerberos authentication and ticket renewal issues on Windows Server 2012 R2 - Out-of-band - Windows 8.1 - KB4594439 (x64)
459443902	4594439: Kerberos authentication and ticket renewal issues on Windows Server 2012 R2 - Out-of-band - Windows Server 2012 R2 - KB4594439 (x64)
459443903	4594439: Kerberos authentication and ticket renewal issues on Windows Server 2012 R2 - Out-of-band - Windows 8.1 - KB4594439
459827501	MS21-JAN: Security Only Quality Update - Security Only - Windows 8.1 - KB4598275 (x64)
459827505	MS21-JAN: Security Only Quality Update - Security Only - Windows 8.1 - KB4598275
459828901	MS21-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4598289 (x64)
459828907	MS21-JAN: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4598289
460127515	4601275: Update for Windows 8.1 - Windows 8.1 - KB4601275 (x64)
460127517	4601275: Update for Windows 8.1 - Windows 8.1 - KB4601275

460134901	MS21-FEB: Security Only Quality Update - Security Only - Windows 8.1 - KB4601349 (x64)
460134905	MS21-FEB: Security Only Quality Update - Security Only - Windows 8.1 - KB4601349
460136303	MS21-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4601363 (x64)
460136305	MS21-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB4601363
460295813	MS21-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 4.8 - KB4601089
460295815	MS21-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4601090
460295817	MS21-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 4.8 - KB4601089 (x64)
460295819	MS21-FEB: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4601090 (x64)
460296001	MS21-FEB: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB4601092 (x64)
460296003	MS21-FEB: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4601094
460296005	MS21-FEB: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB4601092
460296007	MS21-FEB: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4601094 (x64)
460300218	MS21-MAR: Security and Quality Rollup - Windows 7 SP1 (Embedded) - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4600945 (x64) (V2.0)
460300222	MS21-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 (Embedded) - .NET Framework 3.5.1 - KB4578952 (x64)
460300226	MS21-MAR: Security and Quality Rollup - Windows 7 SP1 (Embedded) - .NET Framework 4.8 - KB4600944 (V2.0)
460300228	MS21-MAR: Security and Quality Rollup - Windows 7 SP1 (Embedded) - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4600945 (V2.0)
460300230	MS21-MAR: Security and Quality Rollup - Windows 7 SP1 (Embedded) - .NET Framework 4.8 - KB4600944 (x64) (V2.0)
460300239	MS21-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 (Embedded) - .NET Framework 3.5.1 - KB4578952
460300241	MS21-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 (Embedded) - .NET Framework 4.8 - KB4600944
460300245	MS21-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 (Embedded) - .NET Framework 4.8 - KB4600944 (x64)

460300410	MS21-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 3.5 - KB4578953
460300412	MS21-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.5.2 - KB4578956
460300414	MS21-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 3.5 - KB4578953 (x64)
460300416	MS21-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.5.2 - KB4578956 (x64)
460300425	MS21-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4601048
460300427	MS21-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.8 - KB4601058
460300435	MS21-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.8 - KB4601058 (x64)
460300437	MS21-FEB: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB4601048 (x64)
500085101	MS21-MAR: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB5000851 (x64)
500085105	MS21-MAR: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB5000851
500085301	MS21-MAR: Security Only Quality Update - Security Only - Windows 8.1 - KB5000853 (x64)
500085305	MS21-MAR: Security Only Quality Update - Security Only - Windows 8.1 - KB5000853
500139201	MS21-APR: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB5001392 (x64)
500139205	MS21-APR: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB5001392
500139301	MS21-APR: Security Only Quality Update - Security Only - Windows 8.1 - KB5001393 (x64)
500139305	MS21-APR: Security Only Quality Update - Security Only - Windows 8.1 - KB5001393
500163901	5001639: Update for Windows 7 - Windows 7 SP1 (Embedded) - KB5001639 (x64)
500163905	5001639: Update for Windows 7 - Windows 7 SP1 (Embedded) - KB5001639
500164001	5001640: Update for Windows 8.1 - Windows 8.1 - KB5001640 (x64)
500164005	5001640: Update for Windows 8.1 - Windows 8.1 - KB5001640
500184305	5001878: Security and Quality Rollup - Windows 7 SP1 (Embedded) - .NET Framework 4.8 - KB5001843
500184307	5001878: Security and Quality Rollup - Windows 7 SP1 (Embedded) - .NET Framework 4.8 - KB5001843 (x64)

500184501	5001881: Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1 - Windows 8.1 - .NET Framework 4.8 - KB5001845 (x64)
500184505	5001881: Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1 - Windows 8.1 - .NET Framework 4.8 - KB5001845
500187811	5001878: Security and Quality Rollup - Windows 7 SP1 (Embedded) - .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1 and 4.7.2 - KB5001848 (x64)
500187815	5001878: Security and Quality Rollup - Windows 7 SP1 (Embedded) - .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1 and 4.7.2 - KB5001848
500188121	5001881: Security and Quality Rollup - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 -KB5001850 (x64)
500188123	5001881: Security and Quality Rollup - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2- KB5001850
500322001	MS21-MAY: Security Only Quality Update - Security Only - Windows 8.1 - KB5003220 (x64)
500322005	MS21-MAY: Security Only Quality Update - Security Only - Windows 8.1 - KB5003220
500322805	MS21-MAY: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB5003228
500322807	MS21-MAY: Security Only Quality Update for Windows 7 - Windows 7 SP1 (Embedded) - KB5003228 (x64)
500368103	MS21-JUN: Security Only Quality Update - Security Only - Windows 8.1 - KB5003681 (x64)
500368105	MS21-JUN: Security Only Quality Update - Security Only - Windows 8.1 - KB5003681
500369401	MS21-JUN: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB5003694 (x64)
500369405	MS21-JUN: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB5003694
500428501	MS21-JUL: Security Only Quality Update - Security Only - Windows 8.1 - KB5004285 (x64)
500428505	MS21-JUL: Security Only Quality Update - Security Only - Windows 8.1 - KB5004285
500430701	MS21-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB5004307 (x64)
500430705	MS21-JUL: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB5004307
500437803	MS21-JUL: Servicing Stack Update for Windows 7 - Windows 7 SP1 (Embedded) - KB5004378 (x64)
500437805	MS21-JUL: Servicing Stack Update for Windows 7 - Windows 7 SP1 (Embedded) - KB5004378
500487105	5004871: Security and Quality Rollup for .NET Framework 4.5.2 for Windows 7 SP1 - Windows 7 SP1 (Embedded) - .NET Framework 4.5.2 - KB4578955 (x64) (V4.0)

500487109	5004871: Security and Quality Rollup for .NET Framework 4.5.2 for Windows 7 SP1 - Windows 7 SP1 (Embedded) - .NET Framework 4.5.2 - KB4578955 (V4.0)
500487111	5004871: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 SP1 - Windows 7 SP1 (Embedded) - .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 - KB5004757 (x64)
500487115	5004871: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 SP1 - Windows 7 SP1 (Embedded) - .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 - KB5004757
500487117	5004871: Security and Quality Rollup for .NET Framework 4.8 for Windows 7 SP1 - Windows 7 SP1 (Embedded) - .NET Framework 4.8 - KB5004755 (x64)
500487121	5004871: Security and Quality Rollup for .NET Framework 4.8 for Windows 7 SP1 - Windows 7 SP1 (Embedded) - .NET Framework 4.8 - KB5004755
500487129	5004871: Security and Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 - Windows 7 SP1 (Embedded) - .NET Framework 3.5.1 - KB4578952 (x64)
500487133	5004871: Security and Quality Rollup for .NET Framework 3.5.1 for Windows 7 SP1 - Windows 7 SP1 (Embedded) - .NET Framework 3.5.1 - KB4578952
500487301	5004873: Security and Quality Rollup for .NET Framework 3.5 - Windows 8.1 - .NET Framework 3.5 - KB4578953 (x64)
500487305	5004873: Security and Quality Rollup for .NET Framework 3.5 - Windows 8.1 - .NET Framework 3.5 - KB4578953
500487307	5004873: Security and Quality Rollup for .NET Framework 4.5.2 - Windows 8.1 - .NET Framework 4.5.2 - KB4578956 (x64)
500487311	5004873: Security and Quality Rollup for .NET Framework 4.5.2 - Windows 8.1 - .NET Framework 4.5.2 - KB4578956
500487315	5004873: Security and Quality Rollup for .NET Framework 4.8 - Windows 8.1 - .NET Framework 4.8 - KB5004754 (x64)
500487317	5004873: Security and Quality Rollup for .NET Framework 4.8 - Windows 8.1 - .NET Framework 4.8 - KB5004754
500487319	5004873: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 - Windows 8.1 - .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 - KB5004759 (x64)
500487323	5004873: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 - Windows 8.1 - .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 - KB5004759
500495103	5004951: Security Only Quality Update for Windows 7 - Windows 7 SP1 (Embedded) - KB5004951 (x64)
500495105	5004951: Security Only Quality Update for Windows 7 - Windows 7 SP1 (Embedded) - KB5004951

500495801	5004958: Security Only Quality Update for Windows 8.1 - Windows 8.1 - KB5004958 (x64)
500495805	5004958: Security Only Quality Update for Windows 8.1 - Windows 8.1 - KB5004958
500508901	MS21-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB5005089 (x64)
500508905	MS21-AUG: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB5005089
500510601	MS21-AUG: Security Only Quality Update - Security Only - Windows 8.1 - KB5005106 (x64)
500510605	MS21-AUG: Security Only Quality Update - Security Only - Windows 8.1 - KB5005106
500539101	5005391: Update for Windows 8.1 - Windows 8.1 - KB5005391 (x64)
500539105	5005391: Update for Windows 8.1 - Windows 8.1 - KB5005391
500539203	5005392: Update for Windows 7 - Windows 7 SP1 (Embedded) - KB5005392 (x64)
500539205	5005392: Update for Windows 7 - Windows 7 SP1 (Embedded) - KB5005392
500561501	MS21-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB5005615 (x64)
500561505	MS21-SEP: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB5005615
500562701	MS21-SEP: Security Only Quality Update - Security Only - Windows 8.1 - KB5005627 (x64)
500562705	MS21-SEP: Security Only Quality Update - Security Only - Windows 8.1 - KB5005627
500667107	MS21-OCT: Cumulative Security Update for Internet Explorer 11 - Windows 7 SP1 (Embedded) - IE 11 - KB5006671 (x64)
500667111	MS21-OCT: Cumulative Security Update for Internet Explorer 11 - Windows 7 SP1 (Embedded) - IE 11 - KB5006671
500672801	MS21-OCT: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB5006728 (x64)
500672803	MS21-OCT: Security Only Quality Update - Security Only - Windows 7 SP1 (Embedded) - KB5006728
500672901	MS21-OCT: Security Only Quality Update - Security Only - Windows 8.1 - KB5006729 (x64)
500672905	MS21-OCT: Security Only Quality Update - Security Only - Windows 8.1 - KB5006729
500674301	MS21-OCT: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 (Embedded) - KB5006743 (x64)
500674305	MS21-OCT: Security Monthly Quality Rollup - Monthly Rollup - Windows 7 SP1 (Embedded) - KB5006743

500674901	MS21-OCT: Servicing Stack Update for Windows 7 - Windows 7 SP1 (Embedded) - KB5006749 (x64)
500674905	MS21-OCT: Servicing Stack Update for Windows 7 - Windows 7 SP1 (Embedded) - KB5006749
500676111	5006761: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1 for Windows 7 for x64 - Windows 7 SP1 (Embedded) - KB5006061 (x64)
500676115	5006761: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 7 - Windows 7 SP1 (Embedded) - KB5006061
500676117	5006761: Security and Quality Rollup for .NET Framework 4.8 for Windows 7 - Windows 7 SP1 (Embedded) - .NET Framework 4.8 - KB5006060 (x64)
500676121	5006761: Security and Quality Rollup for .NET Framework 4.8 for Windows 7 - Windows 7 SP1 (Embedded) - .NET Framework 4.8 - KB5006060
500676301	5006064: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 for x64 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB5006064 (x64)
500676303	5006067: Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1 for x64 - Windows 8.1 - .NET Framework 4.8 - KB5006067 (x64)
500676305	5006064: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB5006064
500676307	5006067: Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1 - Windows 8.1 - .NET Framework 4.8 - KB5006067
500725503	MS21-NOV: Security Only Quality Update - Security Only - Windows 8.1 - KB5007255 (x64)
500725505	MS21-NOV: Security Only Quality Update - Security Only - Windows 8.1 - KB5007255
500730119	5007301: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 - Windows 8.1 - NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB5007157 (x64)
500730123	5007301: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 - Windows 8.1 - NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB5007157
500828503	MS21-DEC: Security Only Quality Update - Security Only - Windows 8.1 - KB5008285 (x64)
500828505	MS21-DEC: Security Only Quality Update - Security Only - Windows 8.1 - KB5008285
500860303	5008603: Update for Windows 8.1 - Windows 8.1 - KB5008603 (x64)
500860305	5008603: Update for Windows 8.1 - Windows 8.1 - KB5008603

500886801	MS22-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 3.5 - KB5008868 (x64)
500886805	MS22-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 3.5 - KB5008868
500887001	MS22-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.5.2 - KB5008870 (x64)
500887005	MS22-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.5.2 - KB5008870
500887503	MS22-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB5008875 (x64)
500887505	MS22-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB5008875
500888301	MS22-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.8 - KB5008883 (x64)
500888305	MS22-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.8 - KB5008883
500889103	MS22-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB5008891 (x64)
500889105	MS22-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB5008891
500889303	MS22-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB5008893 (x64)
500889305	MS22-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.5.2 - KB5008893
500889501	MS22-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB5008895 (x64)
500889505	MS22-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB5008895
500889701	MS22-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB5008897 (x64)
500889705	MS22-JAN: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB5008897
500959501	MS22-JAN: Security Only Quality Update - Security Only - Windows 8.1 - KB5009595 (x64)
500959505	MS22-JAN: Security Only Quality Update for Windows 8.1 - Windows 8.1 - KB5009595
501021501	5010215: Update for Windows 8.1 - Windows 8.1 - KB5010215 (x64)
501021505	5010215: Update for Windows 8.1 - Windows 8.1 - KB5010215
501039503	MS22-FEB: Security Only Quality Update - Security Only - Windows 8.1 - KB5010395 (x64)
501039505	MS22-FEB: Security Only Quality Update - Security Only - Windows 8.1 - KB5010395

501058325	5010583: Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB5010462 (x64)
501058329	5010583: Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB5010462
501058333	5010583: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB5010465 (x64)
501058335	5010583: Security and Quality Rollup for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB5010465
501079401	5010794: Update for Windows 8.1 - Windows 8.1 - KB5010794 (x64)
501079405	5010794: Update for Windows 8.1 - Windows 8.1 - KB5010794
501126103	5011261: Update for .NET Framework 4.5.2 for Windows 8.1- Windows 8.1 - .NET Framework 4.5.2 - KB5011261 (x64)
501126105	5011261: Update for .NET Framework 4.5.2 for Windows 8.1 - Windows 8.1 - .NET Framework 4.5.2 - KB5011261
501126303	5011263: Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1- Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB5011263 (x64)
501126305	5011263: Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB5011263
501126601	5011266: Update for .NET Framework 4.8 for Windows 8.1 - Windows 8.1 - .NET Framework 4.8 - KB5011266 (x64)
501126605	5011266: Update for .NET Framework 4.8 for Windows 8.1 - Windows 8.1 - .NET Framework 4.8 - KB5011266
501156001	MS22-MAR: Security Only Quality Update - Security Only - Windows 8.1 - KB5011560 (x64)
501156005	MS22-MAR: Security Only Quality Update - Security Only - Windows 8.1 - KB5011560
501217033	MS22-AUG: Security Update for Windows 8.1 - Windows 8.1 - KB5012170 (x64)
501217037	MS22-AUG: Security Update for Windows 8.1 - Windows 8.1 - KB5012170
501232603	MS22-APR: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB5012147(x64)
501232605	MS22-APR: Security Only Update for .NET Framework 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 -KB5012147
501232609	MS22-APR: Security Only Update for .NET Framework 3.5 for Windows 8.1 - Windows 8.1 - .NET Framework 3.5 - KB5012152(x64)

501232613	MS22-APR: Security Only Update for .NET Framework 4.8 for Windows 8.1 - Windows 8.1 - .NET Framework 4.8 - KB5012144 (x64)
501232617	MS22-APR: Security Only Update for .NET Framework 4.8 for Windows 8.1 - Windows 8.1 - .NET Framework 4.8 - KB5012144
501232619	MS22-APR: Security Only Update for .NET Framework 3.5 for Windows 8.1 - Windows 8.1 for 32-bit systems - .NET Framework 3.5 - KB5012152
501232621	MS22-APR: Security Only Update for .NET Framework 4.5.2 for Windows 8.1 - Windows 8.1 - .NET Framework 4.5.2 - KB5012155 (x64)
501232623	MS22-APR: Security Only Update for .NET Framework 4.5.2 for Windows 8.1 - Windows 8.1 - .NET Framework 4.5.2 - KB5012155
501233101	MS22-APR: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.8 - KB5012124
501233103	MS22-APR: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.8 - KB5012124 (x64)
501233107	MS22-APR: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1- .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB5012130 (x64)
501233117	MS22-APR: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 3.5 - KB5012139(x64)
501233119	MS22-APR: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 3.5 - KB5012139
501233127	5012331: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 - KB5012130
501233137	5012331: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.5.2 - KB5012142 (x64)
501233139	5012331: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.5.2 - KB5012142
501263901	MS22-APR: Security Only Quality Update - Security Only - Windows 8.1 - KB5012639 (x64)
501263905	MS22-APR: Security Only Quality Update - Security Only - Windows 8.1 - KB5012639
501383921	MS22-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB5013621
501383923	MS22-MAY: Security Only Update for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 - Windows 8.1 - .NET Framework 4.6.2/4.7/4.7.1/4.7.2 - KB5013623
501383925	MS22-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB5013616
501383931	MS22-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 3.5 - KB5013621 (x64)
501383937	MS22-MAY: Security Only Update for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 - Windows 8.1 - .NET Framework 4.6.2/4.7/4.7.1/4.7.2 - KB5013623 (x64)

501383941	MS22-MAY: Security Only Quality Update - Security Only - Windows 8.1 - .NET Framework 4.8 - KB5013616 (x64)
501387219	MS22-MAY: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 3.5 - KB5013638
501387221	MS22-MAY: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.6.2/4.7/4.7.1/4.7.2 - KB5013643
501387223	MS22-MAY: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.8 - KB5013631
501387225	MS22-MAY: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 3.5 - KB5013638 (x64)
501387231	MS22-MAY: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.6.2/4.7/4.7.1/4.7.2 - KB5013643 (x64)
501387235	MS22-MAY: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.8 - KB5013631 (x64)
501400103	MS22-MAY: Security Only Quality Update - Security Only - Windows 8.1 - KB5014001 (x64)
501400105	MS22-MAY: Security Only Quality Update - Security Only - Windows 8.1 - KB5014001
501474603	MS22-JUN: Security Only Quality Update - Security Only - Windows 8.1 - KB5014746 (x64)
501474605	MS22-JUN: Security Only Quality Update - Security Only - Windows 8.1 - KB5014746
501498603	5014986: Update for Windows 8.1 - Windows 8.1 - KB5014986 (x64)
501498605	5014986: Update for Windows 8.1 - Windows 8.1 - KB5014986
501587703	MS22-JUL: Security Only Quality Update - Security Only - Windows 8.1 - KB5015877 (x64)
501587705	MS22-JUL: Security Only Quality Update - Security Only - Windows 8.1 - KB5015877
501656813	MS22-JUL: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.6.2/4.7/4.7.1/4.7.2 - KB5014637 (x64)
501656815	MS22-JUL: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.8 - KB5014633 (x64)
501656821	MS22-JUL: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.8 - KB5014633
501656823	MS22-JUL: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 4.6.2/4.7/4.7.1/4.7.2 - KB5014637
501668303	MS22-AUG: Security Only Quality Update - Security Only - Windows 8.1 - KB5016683 (x64)
501668305	MS22-AUG: Security Only Quality Update - Security Only - Windows 8.1 - KB5016683
501674007	5016740: Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB5016370 (x64)

501674011	5016740: Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB5016370
501674013	5016740: Security and Quality Rollup for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6.2 - KB5016372 (x64)
501674017	5016740: Security and Quality Rollup for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6.2 - KB5016372
501722003	5017220: Extended Security Updates (ESU) Licensing Preparation Package for Windows 8.1 - Windows 8.1 - KB5017220 (x64)
501722005	5017220: Extended Security Updates (ESU) Licensing Preparation Package for Windows 8.1 - Windows 8.1 - KB5017220
501736501	MS22-SEP: Security Only Quality Update - Security Only - Windows 8.1 - KB5017365 (x64)
501736505	MS22-SEP: Security Only Quality Update - Security Only - Windows 8.1 - KB5017365
501753113	5017531: Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB5017038 (x64)
501753117	5017531: Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB5017038
501847603	MS22-OCT: Security Only Quality Update - Security Only - Windows 8.1 - KB5018476 (x64)
501847605	MS22-OCT: Security Only Quality Update - Security Only - Windows 8.1 - KB5018476
501892203	MS22-OCT: Servicing Stack Update for Windows 8.1 - Windows 8.1 - KB5018922 (x64)
501892205	MS22-OCT: Servicing Stack Update for Windows 8.1 - Windows 8.1 - KB5018922
501995811	MS22-NOV: Cumulative Security Update for Internet Explorer 11 for Windows 8.1 for x64-based systems - Windows 8.1 - IE 11 - KB5019958 (x64)
501995813	MS22-NOV: Cumulative Security Update for Internet Explorer 11 for Windows 8.1 for x86-based systems - Windows 8.1 - IE 11 - KB5019958
502001001	MS22-NOV: Security Only Quality Update - Security Only - Windows 8.1 - KB5020010 (x64)
502001005	MS22-NOV: Security Only Quality Update - Security Only - Windows 8.1 - KB5020010
502044703	5020447: Update for Windows 8.1 - Windows 8.1 - KB5020447 (x64)
502044705	5020447: Update for Windows 8.1 - Windows 8.1 - KB5020447

502068005	MS22-NOV: Security Only Update for .NET Framework 4.8 for Windows 8.1 - Windows 8.1 - .NET Framework 4.8 - KB5020608 (x64)
502068007	MS22-NOV: Security Only Update for .NET Framework 4.8 for Windows 8.1 - Windows 8.1 - .NET Framework 4.8 - KB5020608
502068009	MS22-NOV: Security Only Update for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 - Windows 8.1 - .NET Framework 4.6.2/4.7/4.7.1/4.7.2 - KB5020611 (x64)
502068011	MS22-NOV: Security Only Update for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 - Windows 8.1 - .NET Framework 4.6.2/4.7/4.7.1/4.7.2 - KB5020611
502069003	MS22-NOV: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 3.5 - KB5016268 (x64)
502069005	MS22-NOV: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - .NET Framework 3.5 - KB5016268
502108101	MS22-DEC: Security Only Update for .NET Framework 3.5 for Windows 8.1 - Windows 8.1 - .NET Framework 3.5 - KB5020897 (x64)
502108105	MS22-DEC: Security Only Update for .NET Framework 3.5 for Windows 8.1 - Windows 8.1 - .NET Framework 3.5 - KB5020897
502108107	MS22-DEC: Security Only Update for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 - Windows 8.1 - .NET Framework 4.6.2/4.7/4.7.1/4.7.2 - KB5020899 (x64)
502108111	MS22-DEC: Security Only Update for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 - Windows 8.1 - .NET Framework 4.6.2/4.7/4.7.1/4.7.2 - KB5020899
502108115	MS22-DEC: Security Only Update for .NET Framework 4.8 for Windows 8.1 - Windows 8.1 - .NET Framework 4.8 - KB5020902(x64)
502108117	MS22-DEC: Security Only Update for .NET Framework 4.8 for Windows 8.1 - Windows 8.1 - .NET Framework 4.8 - KB5020902
502109301	MS22-DEC: Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB5020862 (x64)
502109305	MS22-DEC: Security and Quality Rollup for .NET Framework 3.5 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 3.5 - KB5020862
502109309	MS22-DEC: Security and Quality Rollup for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6.2 - KB5020868 (x64)
502109311	MS22-DEC: Security and Quality Rollup for .NET Framework 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.6.2 - KB5020868
502109315	MS22-DEC: Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB5020878(x64)

502109317	MS22-DEC: Security and Quality Rollup for .NET Framework 4.8 for Windows 8.1, RT 8.1, and Windows Server 2012 R2 - Windows 8.1 - .NET Framework 4.8 - KB5020878
502129603	MS22-DEC: Security Only Quality Update - Security Only - Windows 8.1 - KB5021296 (x64)
502129605	MS22-DEC: Security Only Quality Update - Security Only - Windows 8.1 - KB5021296
502165301	5021653: Update for Windows 8.1 - Windows 8.1 - KB5021653 (x64)
502165305	5021653: Update for Windows 8.1 - Windows 8.1 - KB5021653
502234601	MS23-JAN: Security Only Quality Update - Security Only - Windows 8.1 - KB5022346 (x64)
502234605	MS23-JAN: Security Only Quality Update - Security Only - Windows 8.1 - KB5022346
502235201	MS23-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - KB5022352 (x64)
502235205	MS23-JAN: Security Monthly Quality Rollup - Monthly Rollup - Windows 8.1 - KB5022352
2004032501	Update: Service Pack 6 for Visual Basic 6.0 - Windows XP SP3 / Windows 2003 SP2(Superseded)