

IBM BigFix
CVE Dashboard
Installation Guide

Table of Contents

What's This?	3
Quick Start	3
What it looks like	4
Step-By-Step Install Guide	5
1. Download and unzip the package	5
2. Run the import utility (bigfix_cve_util.exe).....	5
3. Load the Dashboard into the BigFix Console	6
For Interest	10

BigFix CVE Dashboard

What's This?

This is a BigFix Console based dashboard to view **Common Vulnerabilities & Exposures (CVE)** information as correlated with BigFix Fixlets and affected computers.

Many security professionals manage risks and vulnerabilities by tracking and monitoring CVEs as published by MITRE.

CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known cyber security issues. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this "common enumeration."

This BigFix CVE Dashboard is comprised of 2 components:

- A command-line utility that downloads, correlates, then imports CVE information from **National Vulnerability Database (NVD)** into BigFix. This utility can be run using a Fixlet that is provided.
- A BigFix Console based dashboard for searching, viewing, and exporting the results.

Quick Start

1. Download and unzip BigFix CVE Dashboard in any folder. [Download Link](#).
2. Run the bigfix_cve_util.exe to download the CVEs from NVD and post to BigFix (This takes a long time, > 30 minutes).
(Once tested, this utility can be executed on a schedule using the [Fixlet](#) provided)
3. In the BigFix Console --> Debug menu --> Load Wizard and find the CVEs.ojo file
The Debug menu in the Console is turned on by simultaneously pressing Ctrl-Alt-Shift-D then check Show Debug Menu.

Using "Load Wizard" imports the dashboard temporarily and it will be removed upon Console exit.
You can add the Dashboard to a custom site using Console menu --> Tools --> Add Files to Site...

IBM BigFix CVE Dashboard

What it looks like

The screenshot displays the IBM BigFix CVE Dashboard interface. The main content area shows a table of vulnerabilities from the National Vulnerability Database. The table includes columns for CVE ID, Published Date, Source, CVSS Score, Related Fixlets, Vulnerable Computers, Total Computers, Cumulative Score, CVE Compliance, and Summary. The dashboard also features a left-hand navigation menu with categories like All Content, BigFix Management, Endpoint Protection, Patch Management, Security Configuration, Server Automation, Systems Lifecycle, and BigFix Labs. At the top, there are filters for Year (All), CVSS Score (High 7.0@9), and Vulnerable Computers (0). The data is imported from 2016-04-11 17:26:10 -07:00.

CVE ID	Published Date	Source	CVSS Score	Related Fixlets	Vulnerable Computers	Total Computers	Cumulative Score	CVE Compliance	Summary
CVE-2016-0010	2016-01-13	Microsoft	9.3	18	1	516	9.3	99.8%	Microsoft Office 2007 SP3, Office 2010 SP2, Office 2013 SP1, Office 2013 RT SP1, Office 2016, Excel for Mac 2011, PowerPoint for Mac 2011, Word for Mac 2011, Excel 2016 for Mac, PowerPoint 2016 for Mac, Word 2016 for Mac, and Word Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."
CVE-2016-0021	2016-03-09	Microsoft	9.3	8	1	464	9.3	99.8%	Microsoft InfoPath 2007 SP3, 2010 SP2, and 2013 SP1 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."
CVE-2016-0054	2016-02-10	Microsoft	9.3	24	1	516	9.3	99.8%	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 2016 for Mac, Office Compatibility Pack SP3, Excel Viewer, Excel Services on SharePoint Server 2007 SP3, Excel Services on SharePoint Server 2010 SP2, Excel Services on SharePoint Server 2013 SP1, and Office Web Apps 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."
CVE-2016-0057	2016-03-09	Microsoft	7.2	4	1	464	7.2	99.8%	Microsoft Office 2007 SP3, 2010 SP2, 2013 SP1, and 2016 does not properly sign an unspecified binary file, which allows local users to gain privileges via a Trojan horse file with a crafted signature, aka "Microsoft Office Security Feature Bypass Vulnerability."
CVE-2016-0134	2016-03-09	Microsoft	9.3	26	1	516	9.3	99.8%	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Word for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, Word Viewer, Word Automation Services on SharePoint Server 2010 SP2 and 2013 SP1, Office Web Apps 2010 SP2, and Web Apps Server 2013 SP1 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."
CVE-2016-0636	2016-03-24	Oracle	9.3	10	1	516	9.3	99.8%	Unspecified vulnerability in Oracle Java SE 7u97, 8u73, and 8u74 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to the Hotspot sub-component.
CVE-2016-0936	2016-01-14	Adobe	9.3	5	1	516	9.3	99.8%	Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.20119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted PDF data, a different vulnerability than CVE-2016-0931, CVE-2016-0933, CVE-2016-0938, CVE-2016-0939, CVE-2016-0942, CVE-2016-0944, CVE-2016-0945, and CVE-2016-0946.
CVE-2016-0937	2016-01-14	Adobe	9.3	5	1	516	9.3	99.8%	Use-after-free vulnerability in the OGG object implementation in Adobe Reader and Acrobat before 11.0.14, Acrobat and Acrobat Reader DC Classic before 15.006.20119, and Acrobat and Acrobat Reader DC Continuous before 15.010.20056 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0932, CVE-2016-0934, CVE-2016-0940, and CVE-2016-0941.
CVE-2010-1387	2010-06-18	oval.mitre.org	9.3	1	1	464	9.3	99.8%	Use-after-free vulnerability in Java ScriptCore in WebKit in Apple iTunes before 9.2 on Windows, and Apple iOS before 4 on the iPhone and iPod touch, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via vectors related to page transitions, a different vulnerability than CVE-2010-1763 and CVE-2010-1769.
CVE-2016-0940	2016-04-01	Apple	7.5	6	1	600	7.5	99.8%	Unspecified vulnerability in the Java 2D component in Oracle Java SE and Java for Business 6 Update 10, 5.0 Update 23, 1.4.2_25, and 1.3.1_27 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors. NOTE: the previous information was obtained from the March 2010 CPU.

Step-By-Step Install Guide

1. Download and unzip the package

[Download the zip file CVEDashboard.zip](#) and unzip to any location.

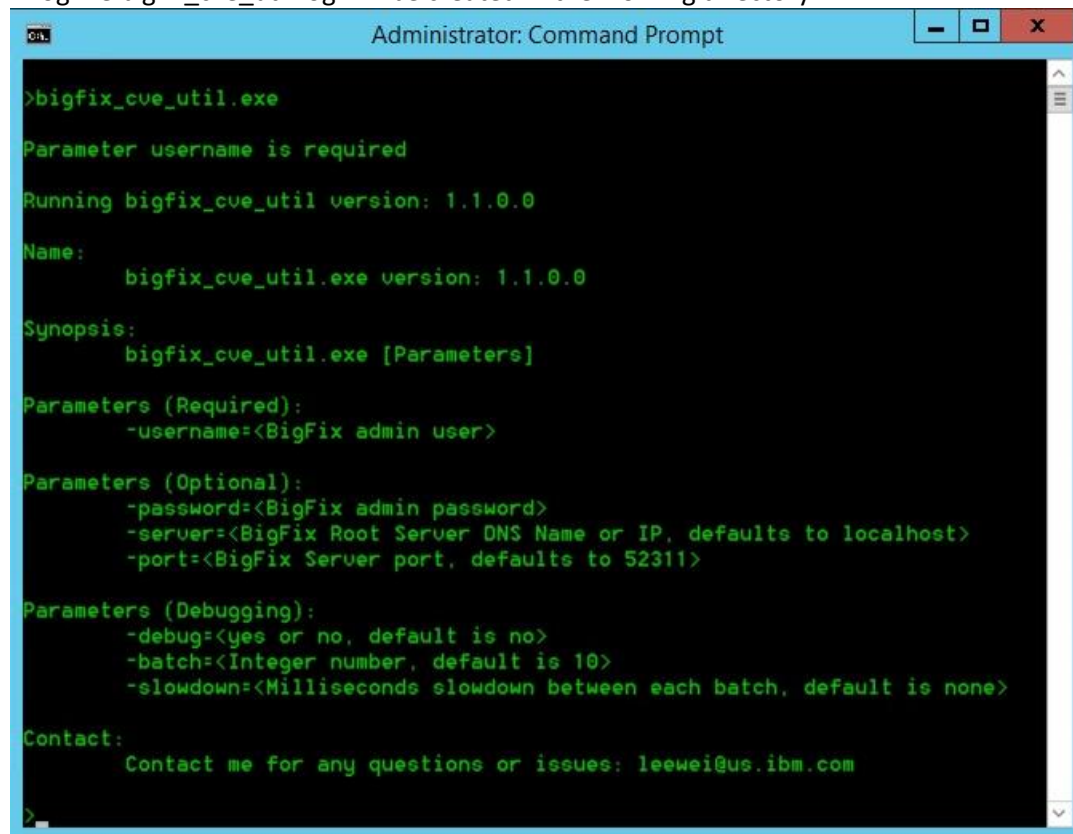
2. Run the import utility (bigfix_cve_util.exe)

Run the \importer\bigfix_cve_util.exe.

- The utility downloads the CVE data from the [National Vulnerability Database](#) (NVD) by year (2009 – 2016)
- It correlates the CVE numbers against any Fixlets already in the BigFix repository
- The utility posts the results into BigFix via the REST API

```
C:\> bigfix_cve_util.exe -server=bigfix.company.com -port=52311  
-username=bigfixadmin
```

A log file bigfix_cve_util.log will be created in the working directory.



```
Administrator: Command Prompt  
>bigfix_cve_util.exe  
Parameter username is required  
Running bigfix_cve_util version: 1.1.0.0  
Name:  
    bigfix_cve_util.exe version: 1.1.0.0  
Synopsis:  
    bigfix_cve_util.exe [Parameters]  
Parameters (Required):  
    -username=<BigFix admin user>  
Parameters (Optional):  
    -password=<BigFix admin password>  
    -server=<BigFix Root Server DNS Name or IP, defaults to localhost>  
    -port=<BigFix Server port, defaults to 52311>  
Parameters (Debugging):  
    -debug=<yes or no, default is no>  
    -batch=<Integer number, default is 10>  
    -slowdown=<Milliseconds slowdown between each batch, default is none>  
Contact:  
    Contact me for any questions or issues: leewei@us.ibm.com  
>
```

IBM BigFix CVE Dashboard

Once tested, this utility can be executed from a Fixlet on a schedule. The default schedule is to run this once a day to retrieve new CVEs published, as well as to update computers affected by the CVEs.

- Download the Task: [Schedule National Vulnerability Database \(NVD\) CVE Import.bes](#)
- Save the Task anywhere on disk
- Double-click to import into the BigFix Console
- Take action and target one computer designated as the import computer. Any Windows computer with an Internet access (to download the XML files from NVD) and a connection to the BigFix Server will work. The connection to the BigFix Server is done via HTTPS REST API.

The screenshot shows the 'Create Task' dialog box in the BigFix Console. The dialog is titled 'Create Task' and has a blue header. The 'Name' field contains 'Schedule National Vulnerability Database (NVD) CVE Import'. The 'Create in site' dropdown is set to 'Master Action Site' and the 'Create in domain' dropdown is set to 'All Content'. Below the name field are tabs for 'Description', 'Actions', 'Relevance', and 'Properties'. The 'Description' tab is active, showing a rich text editor with the following content: 'Information', 'This task is used to schedule periodical National Vulnerability Database (NVD) CVE data import. The default action is to run the import once a day, but that can be changed as desired.', 'The utility uses the IBM BigFix REST API to import data into the BigFix Server.', 'This Task uses the secure parameters feature to ensure that the credentials entered below are protected. The parameters are encrypted and delivered to the targeted endpoint mailbox. Only the targeted endpoint can access the parameters.', and 'Enter the following required parameters'. Below this text are four input fields: 'BigFix Root Server (FQDN or IP address):', 'BigFix Root Server Port:', 'Username:', and 'Password:'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

3. Load the Dashboard into the BigFix Console

The Dashboard can be loaded into the Console in one of 2 ways. One is temporary and suitable for testing. It goes away after the Console is closed. The other is permanent by adding it to the custom site.

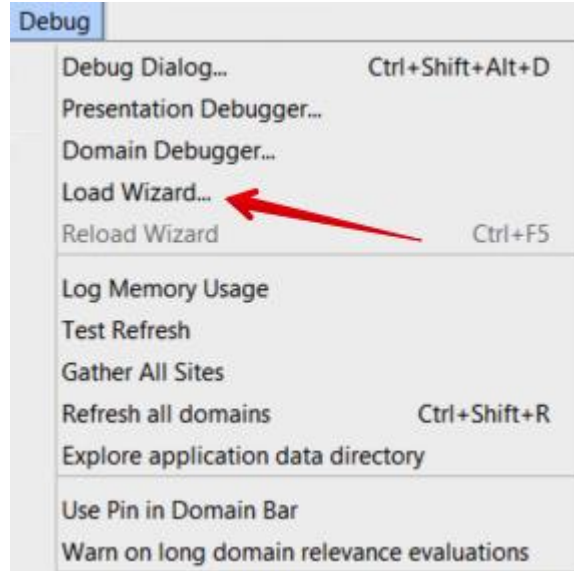
Temporary Testing

For the purpose of testing, the CVE Dashboard can be loaded into the Console.

- Enable the "Debug" menu in BigFix Console. This is done by pressing Ctrl-Alt-Shift-D together. Click the "Show Debug Menu" check box to make this appear as a menu item.

IBM BigFix CVE Dashboard

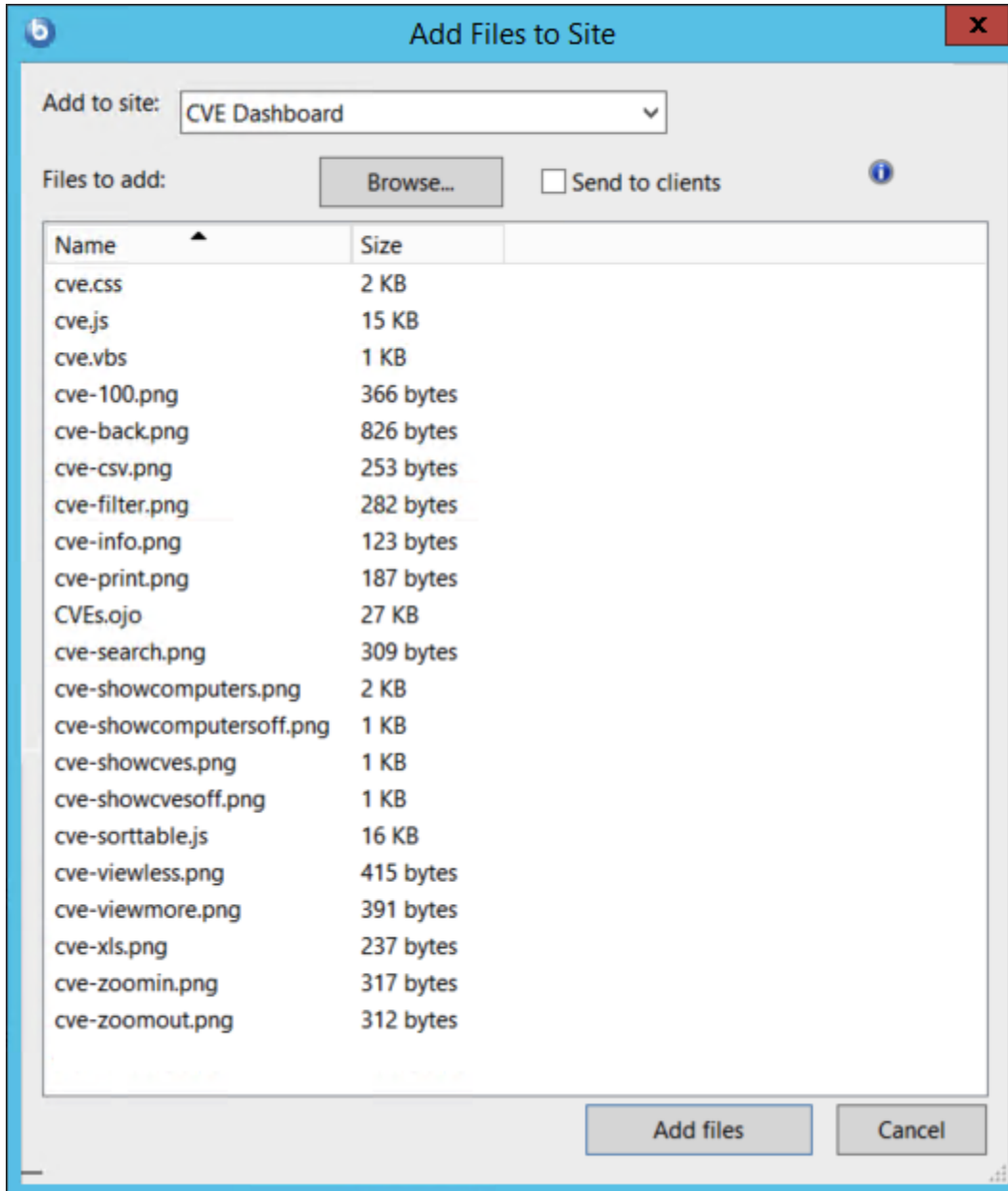
- Use menu option Debug → Load Wizard... and locate the “CVEs.ojo” file downloaded earlier.



Persistent Install

A persistent install of the Dashboard is done by adding all the files to a Custom Site.

- Create a custom site if desired. Or use the Master Action Site. It is preferred to use a custom site.
- This is done with Console menu Tools → Create Custom Site...
- Add the files using Console menu Tools → Add Files to Site...
- Add all the files as shown below. Files in a BigFix site does not have hierarchy, which is why they are all at the same root level.
- If the “Send to clients” checkbox is checked, this means that all these files will be sent to all clients subscribing to this custom site. This is not necessary because most clients will not be using a Console to display the dashboard.
- The Dashboard should now be available in the Console folder Dashboards → All Dashboards → CVEs



IBM BigFix CVE Dashboard

National Vulnerability Database CVE Dashboard v1.1

207 of 207 items | Year: All | CVSS Score > Critical 9.0-10.0 | Vulnerable Computers => 1 | Data imported

CVE ID	Published Date	Source	CVSS Score	Related Fixlets	Vulnerable Computers	Total Computers	Cumulative Score	CVE Compliance	Summary
CVE-2016-1754	2016-03-23	Apple	9.3	4	1	3	9.3	66.7%	The kernel in Apple iOS bef...
CVE-2016-1755	2016-03-23	Apple	9.3	4	1	3	9.3	66.7%	The kernel in Apple iOS bef...
CVE-2016-1759	2016-03-23	Apple	9.3	4	1	3	9.3	66.7%	The kernel in Apple OS X be...
CVE-2016-1778	2016-03-23	Apple	9.3	2	1	3	9.3	66.7%	WebKit in Apple iOS before ...
CVE-2016-1783	2016-03-23	Apple	9.3	2	1	3	9.3	66.7%	WebKit in Apple iOS before ...
CVE-2016-1800	2016-05-20	Apple	9.3	2	1	3	9.3	66.7%	Captive Network Assistant i...
CVE-2016-1846	2016-05-20	Apple	9.3	2	1	3	9.3	66.7%	The NVIDIA Graphics Driver...
CVE-2016-0994	2016-03-12	Adobe Microsoft	9.3	14	2	12	27.9	75.0%	Use-after-free vulnerability ...
CVE-2016-0996	2016-03-12	Adobe Microsoft	9.3	14	2	12	27.9	75.0%	Use-after-free vulnerability ...
CVE-2016-1005	2016-03-12	Adobe Microsoft	9.3	14	2	12	27.9	75.0%	Adobe Flash Player before ...
CVE-2015-1673	2015-05-13	Microsoft oval.mitre.org	9.3	20	2	9	18.6	77.8%	The Windows Forms (aka ...
CVE-2015-2504	2015-09-08	Microsoft	9.3	36	2	9	18.6	77.8%	Microsoft .NET Framework 2...
CVE-2015-6108	2015-12-09	Microsoft	9.3	42	2	9	18.6	77.8%	The Windows font library in...
CVE-2014-4149	2014-11-11	Microsoft oval.mitre.org	9.3	21	2	9	18.6	77.8%	Microsoft .NET Framework 1...
CVE-2016-0936	2016-01-14	Adobe	9.3	5	2	12	18.6	83.3%	Adobe Reader and Acrobat ...

0 items in list, 0 selected. | Connected to 'Maze' as user 'leewei'

For Interest

For reference on April 2016, these are the number of Fixlets with CVE numbers in each sites. These numbers will change over time.

Of the CVEs from 2009 - 2016 being loaded.

CVEs being loaded from NVD	39,548
CVEs with BigFix Fixlets	12,558
% CVEs with BigFix Fixlets	32%

Name of Site	Number of Fixlets with CVE Reference
Patches for AIX	621
Patches for CentOS 5	465
Patches for CentOS 5 Native Tools	688
Patches for CentOS 6	483
Patches for CentOS 6 Native Tools	1,084
Patches for CentOS 7	302
Patches for Debian 7	1,532
Patches for ESX	141
Patches for ESXi	23
Patches for Mac OS X	198
Patches for Oracle Linux 7	1,263
Patches for RHEL 3	296
Patches for RHEL 4	276
Patches for RHEL 5	531
Patches for RHEL 5 - Dependency Resolution	445
Patches for RHEL 6 - Dependency Resolution	690
Patches for RHEL 6 System Z	696
Patches for RHEL 7	289
Patches for RHEL5 - Native Tools	1,230
Patches for RHEL6 - Native Tools	1,989
Patches for RedHat Enterprise Linux	1,974
Patches for RedHat Linux	128
Patches for SLE 11 Native Tools	4,269
Patches for SLE 12 Native Tools	669
Patches for SLE10	893
Patches for SLE10 System Z	227
Patches for SLE11	3,258
Patches for SLE11 System Z	786

IBM BigFix CVE Dashboard

Patches for Solaris	169
Patches for Ubuntu 0804	308
Patches for Ubuntu 1004	1,378
Patches for Ubuntu 1204	1,762
Patches for Ubuntu 1404	958
Patches for Windows	8,353
Patches for Windows (Brazilian Portuguese)	6,402
Patches for Windows (CHT)	6,599
Patches for Windows (Czech)	5,749
Patches for Windows (Danish)	4,783
Patches for Windows (Finnish)	3,960
Patches for Windows (French)	6,694
Patches for Windows (German)	6,649
Patches for Windows (Greek)	3,924
Patches for Windows (Hebrew)	4,785
Patches for Windows (Hungarian)	5,678
Patches for Windows (Italian)	6,535
Patches for Windows (Japanese)	6,984
Patches for Windows (Korean)	6,560
Patches for Windows (NLD)	5,527
Patches for Windows (Norwegian)	3,963
Patches for Windows (Polish)	5,745
Patches for Windows (Russian)	7,702
Patches for Windows (Simplified Chinese)	6,564
Patches for Windows (Spanish)	6,626
Patches for Windows (Swedish)	5,608
Patches for Windows (Turkish)	5,666
Patches for zLinux	390
Updates for Mac Applications	271
Updates for Windows Applications	1,044
Vulnerabilities to Windows Systems	7,624
Windows Point of Sale	597
Total	171,003