HCLSoftware

November 2023 BigFix Briefing Room

Rhonda Studnick Kaiser
&
Don Moss

HCLSoftware

November 2023
BigFix Briefing Room

Today's Agenda

- Intro & greetings
- November Microsoft Patch Details
- Mobile & Wireless
- Microsoft non security updates
- CISA KEV
- Notable Exploits and Malware News
- Announcements & Upcoming Events
- Resources

HCL BigFix

BigFix Briefing Room: Meet Your Hosts

Rhonda Studnick Kaiser

Rhonda is responsible for customer outreach and has impacts cross functionally across the organization from Engineering and Product Management, to Support and Professional Services through networked relationships.

Don Moss

Don is a BigFix Technical Advisor based in Madison Wisconsin. He joined IBM in 2015 and was selected to come over to HCL. Don has supported customers in the mid-west and Canada. He was then selected to support the BigFix Partner program for the past year. Don is now back supporting customers on the West coast as well as continuing to support named accounts for the BigFix partner and channel programs.

HCLSoftware

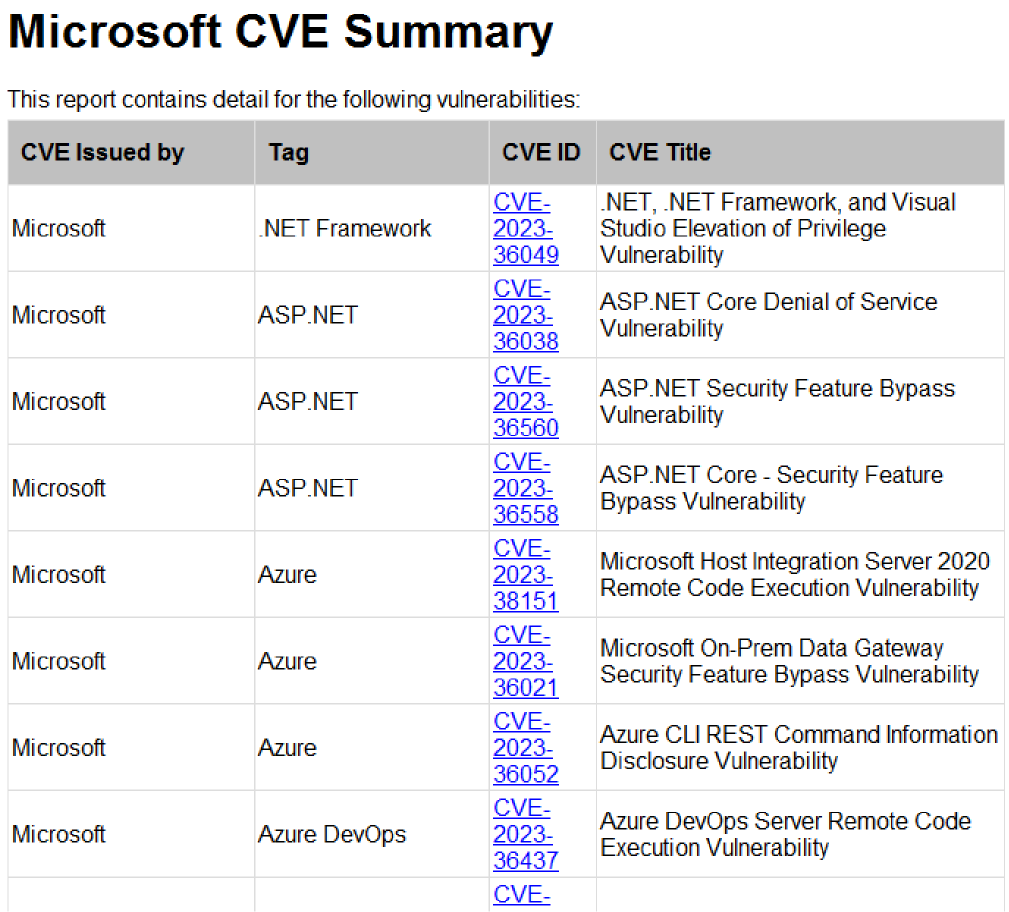
November 2023 Microsoft Updates

Common Vulnerability Exploits (CVE’s)

Don Moss, BigFix Technical Adviser

With the ***October*** forecast for large numbers of CVEs addressed in Windows 10 and 11 and the recent record on the number fixed in Windows Server 2012 was spot on!

So, Microsoft addressed 75 CVEs in Windows 11, 80 in Windows 10, and 61 in Server 2012 R2!



Microsoft CVE Summary

This report contains detail for the following vulnerabilities:

CVE Issued by	Tag	CVE ID	CVE Title
Microsoft	.NET Framework	CVE-2023-36049	.NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability
Microsoft	ASP.NET	CVE-2023-36038	ASP.NET Core Denial of Service Vulnerability
Microsoft	ASP.NET	CVE-2023-36560	ASP.NET Security Feature Bypass Vulnerability
Microsoft	ASP.NET	CVE-2023-36558	ASP.NET Core - Security Feature Bypass Vulnerability
Microsoft	Azure	CVE-2023-38151	Microsoft Host Integration Server 2020 Remote Code Execution Vulnerability
Microsoft	Azure	CVE-2023-36021	Microsoft On-Prem Data Gateway Security Feature Bypass Vulnerability
Microsoft	Azure	CVE-2023-36052	Azure CLI REST Command Information Disclosure Vulnerability
Microsoft	Azure DevOps	CVE-2023-36437	Azure DevOps Server Remote Code Execution Vulnerability
		CVE-	

November 2023 Patch Tuesday forecast

- Expect a smaller number of CVEs addressed next week in the Microsoft operating systems after the big push last month. There may be a bigger focus on the Office applications and perhaps a .NET framework update.
- Adobe has been consistent with major updates at the end of each quarter, so I anticipate the next one in December. If an important zero-day surfaces they may release something next week so always watch for a pre-announcement in the next day or so.
- Apple released security updates for Sonoma, Ventura, and iOS this week so ensure you factor them into your patch deployment for next week if you haven't already. Be on the lookout for a Monterey update just in case some of the CVEs apply to that OS.
- The ChromeOS LTS channel was updated to 114.0.5735.339 this week addressing 5 High rated CVEs. Take those into account next week if you haven't deployed them. There were beta updates this week for Chrome Desktop and standard ChromeOS, so expect those to release next week.
- Mozilla released their last round of updates for Firefox, Firefox ESR and Thunderbird on October 24, so we may see some minor updates next week.

Zero Day Info

The 1st zero-day threat targeting Microsoft this month include CVE-2023-36025, a weakness that allows malicious content to bypass the Windows SmartScreen Security feature. SmartScreen is a built-in Windows component that tries to detect and block malicious websites and files. Microsoft's security advisory for this flaw says attackers could exploit it by getting a Windows user to click on a booby-trapped link to a shortcut file.

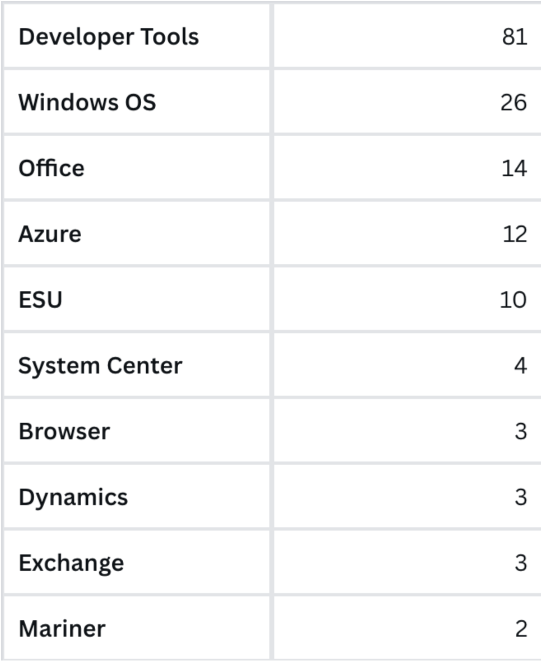
The second zero day this month is CVE-2023-36033, which is a vulnerability in the "DWM Core Library" in Microsoft Windows that was exploited in the wild as a zero day and publicly disclosed prior to patches being available. It affects Microsoft Windows 10 and later, as well as Microsoft Windows Server 2019 and subsequent versions.

The final zero day in this month's Patch Tuesday is a problem in the "Windows Cloud Files Mini Filter Driver" tracked as CVE-2023-36036 that affects Windows 10 and later, as well as Windows Server 2008 at later. Microsoft says it is relatively straightforward for attackers to exploit CVE-2023-36036 as a way to elevate their privileges on a compromised PC.

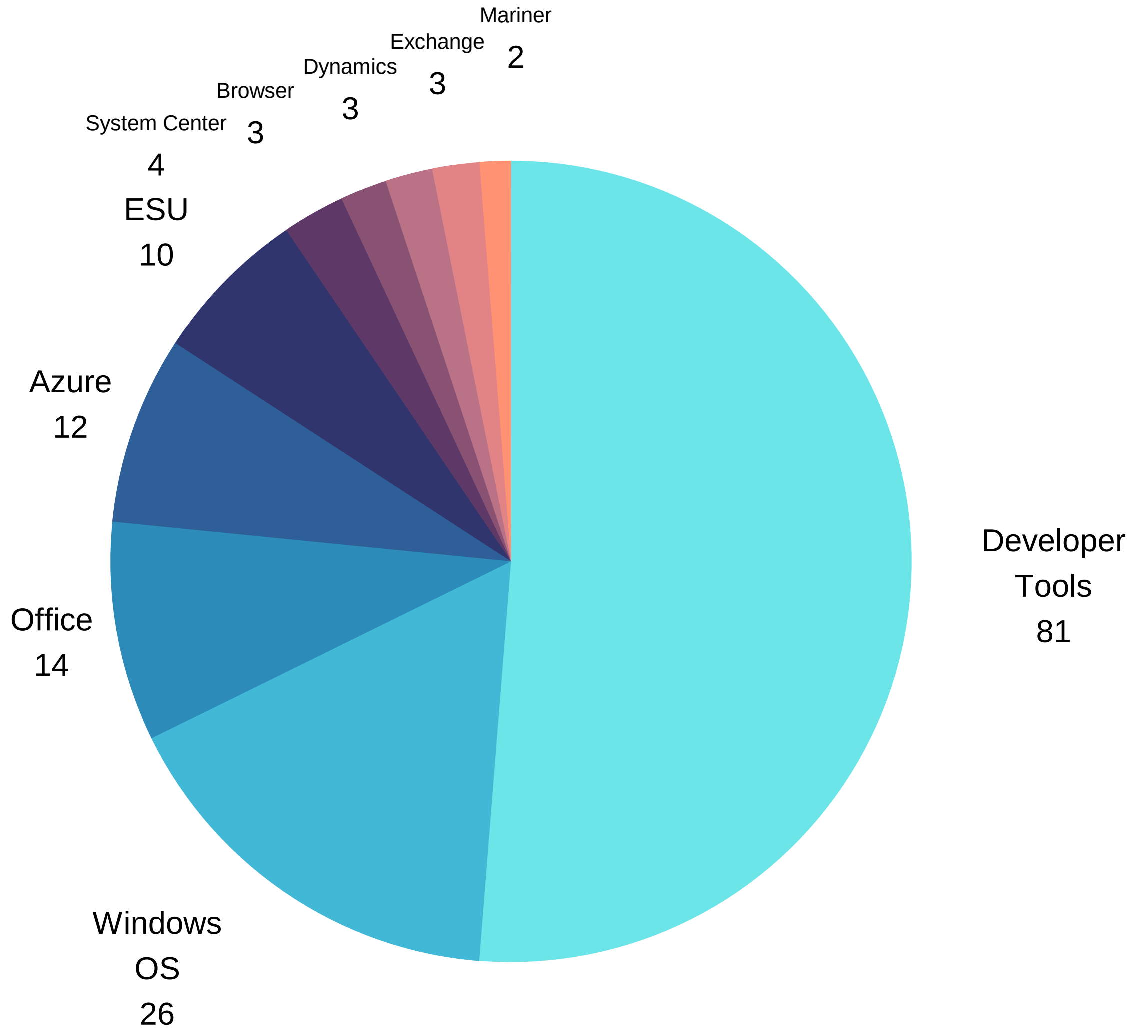
Beyond the zero day flaws, organizations running **Microsoft Exchange Server** should prioritize several new Exchange patches, including CVE-2023-36439, which is a bug that would allow attackers to install malicious software on an Exchange server. This weakness technically requires the attacker to be authenticated to the target's local network, but notes that a pair of phished Exchange credentials will provide that access nicely.

November: 158 MICROSOFT CVE'S

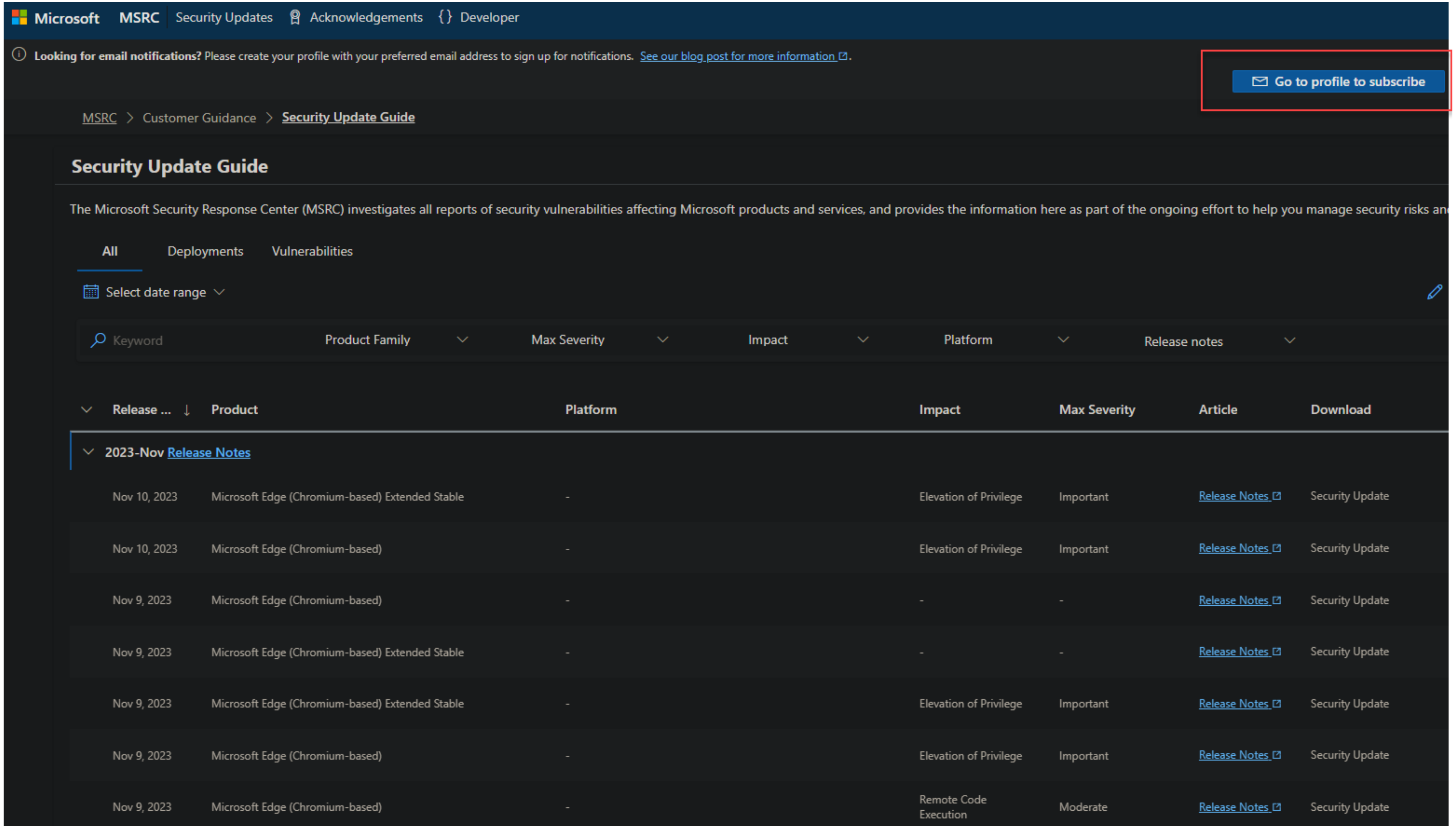
Common Vulnerabilities and Exposures



Developer Tools	81
Windows OS	26
Office	14
Azure	12
ESU	10
System Center	4
Browser	3
Dynamics	3
Exchange	3
Mariner	2



Please check out the Microsoft Security Response Center (MSRC)!



Looking for email notifications? Please create your profile with your preferred email address to sign up for notifications. See our blog post for more information.

MSRC > Customer Guidance > Security Update Guide

Security Update Guide

The Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services, and provides the information here as part of the ongoing effort to help you manage security risks an

Release ... ↓	Product	Platform	Impact	Max Severity	Article	Download
2023-Nov Release Notes						
Nov 10, 2023	Microsoft Edge (Chromium-based) Extended Stable	-	Elevation of Privilege	Important	Release Notes	Security Update
Nov 10, 2023	Microsoft Edge (Chromium-based)	-	Elevation of Privilege	Important	Release Notes	Security Update
Nov 9, 2023	Microsoft Edge (Chromium-based)	-	-	-	Release Notes	Security Update
Nov 9, 2023	Microsoft Edge (Chromium-based) Extended Stable	-	-	-	Release Notes	Security Update
Nov 9, 2023	Microsoft Edge (Chromium-based) Extended Stable	-	Elevation of Privilege	Important	Release Notes	Security Update
Nov 9, 2023	Microsoft Edge (Chromium-based)	-	Elevation of Privilege	Important	Release Notes	Security Update
Nov 9, 2023	Microsoft Edge (Chromium-based)	-	Remote Code Execution	Moderate	Release Notes	Security Update

https://msrc.microsoft.com/update-guide/vulnerability

MOBILE & WIRELESS

37 Vulnerabilities Patched in Android With November 2023 Security Updates

The Android security updates released this week resolve 37 vulnerabilities, including a critical information disclosure bug.

Google on Monday announced patches for 37 vulnerabilities as part of the November 2023 Android security updates, with additional fixes released for Pixel devices.

The first part of the security update will arrive on devices as the *2023-11-01 security patch level*, addressing 15 vulnerabilities in Android's Framework and System components.
"The most severe of these issues is a critical security vulnerability in the System component that could lead to local information disclosure with no additional execution privileges needed," Google notes in its advisory.
The bug is tracked as CVE-2023-40113, impacts Android versions 11, 12, 12L, and 13, and was addressed alongside six other issues in the System component, which are rated 'high severity'.

HCLSoftware

November 2023 non-Security updates

The November 2023 Office non-Security updates have been released and they are not included in the DEFCON-3 approval for the October 2023 patches.
Unless you have a specific need to install them, you should wait until Susan Bradley (Patch Lady) approves them and any problems have been reported.

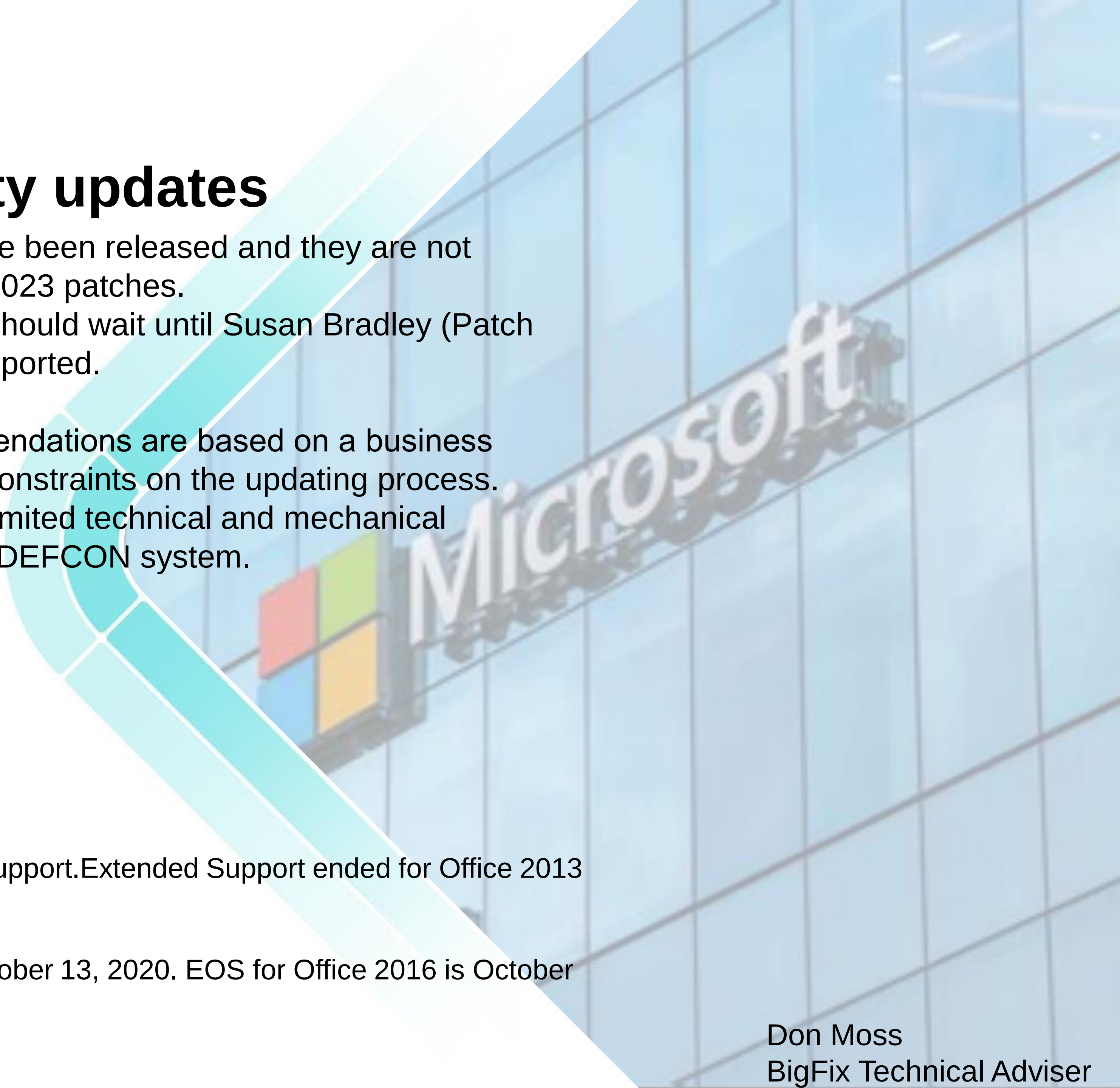
Remember, Susan’s patching sequence and recommendations are based on a business environment that has IT support and may have time constraints on the updating process. Consumer patching should be more cautious due to limited technical and mechanical resources. The latter is the reason for the AskWoody DEFCON system.

Office 2013
Update for Microsoft Outlook 2013 (KB5002514)

Office 2016
Update for Microsoft Outlook 2016 (KB5002523)
Update for Microsoft Project 2016 (KB5002502)

On April 10, 2018, Office 2013 reached End of Mainstream Support.Extended Support ended for Office 2013 on April 11, 2023.

Office 2016 also reached End of Mainstream Support on October 13, 2020. EOS for Office 2016 is October 14, 2025.



Don Moss
BigFix Technical Adviser

HCLSoftware

Notable Exploits,

In Vulnerability Management
November 2023

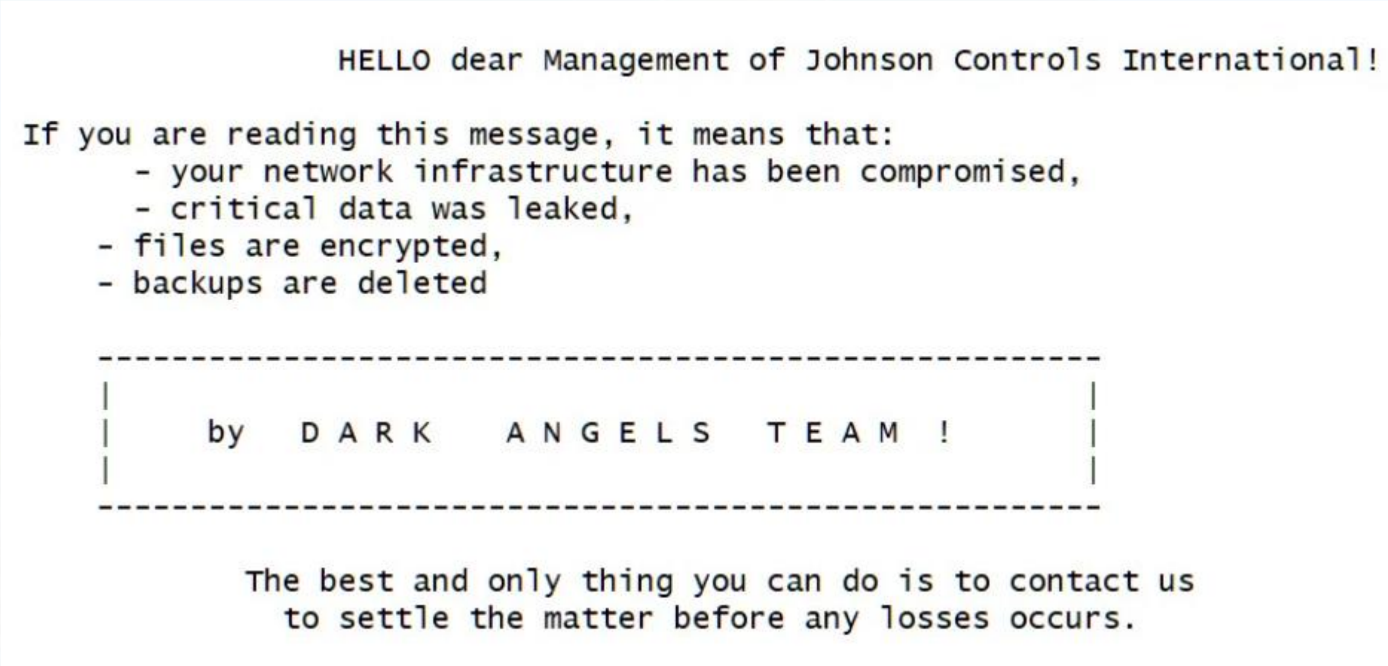
Notable Trends, Exploits & News

November 2023 News

Building automation giant Johnson Controls hit by ransomware attack

The Breach

Johnson Controls International suffered what is described as a massive ransomware attack that encrypted many of the company devices, including VMware ESXi servers, impacting the company's and its subsidiaries' operations. 28 Terabytes of data was stolen – 51 Million sought by Dark Angel Team (APT)



```
                 HELLO dear Management of Johnson Controls International!

If you are reading this message, it means that:
      - your network infrastructure has been compromised,
      - critical data was leaked,
    - files are encrypted,
    - backups are deleted

    ------------------------------------------------------
    |                                                    |
    |     by  D A R K   A N G E L S   T E A M !          |
    |                                                    |
    ------------------------------------------------------

            The best and only thing you can do is to contact us
              to settle the matter before any losses occurs.
```

HCLSoftware

CISA KEV

Cybersecurity & Infrastructure
Security Agency (CISA)

Known Exploited Vulnerabilities (KEV)

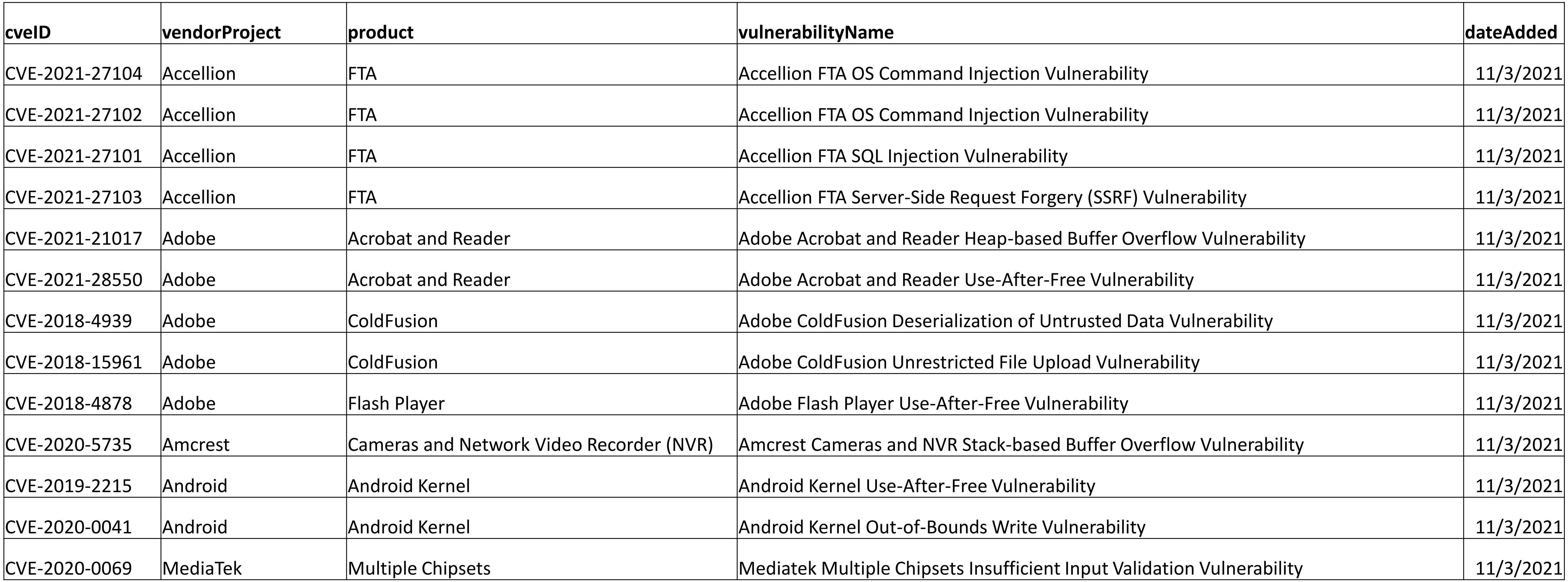
About CISA KEV

Cybersecurity & Infrastructure Security Agency (CISA) | Known Exploited Vulnerabilities (KEV)

- Operational lead for US Federal Cybersecurity and the US National coordinator for Critical Infrastructure Security and Resilience.
- Mission to lead the US national effort to understand, manage, and reduce risk to cyber and physical infrastructure
- Publishes KEV list
- KEV list quickly becoming a leading operational data source for the prioritization of vulnerability remediation efforts across commercial industries
- Takeaway: if your organization doesn’t know where to start with vulnerability remediation efforts, the KEV list is a good place to start. Talk to your BigFix Technical Advisor for additional best practices.

CISA KEV - November 2023 News

CISA.gov has added many new entries to its “Known Exploited Catalog” since Oct. 13 (small sample below)



cveID	vendorProject	product	vulnerabilityName	dateAdded
CVE-2021-27104	Accellion	FTA	Accellion FTA OS Command Injection Vulnerability	11/3/2021
CVE-2021-27102	Accellion	FTA	Accellion FTA OS Command Injection Vulnerability	11/3/2021
CVE-2021-27101	Accellion	FTA	Accellion FTA SQL Injection Vulnerability	11/3/2021
CVE-2021-27103	Accellion	FTA	Accellion FTA Server-Side Request Forgery (SSRF) Vulnerability	11/3/2021
CVE-2021-21017	Adobe	Acrobat and Reader	Adobe Acrobat and Reader Heap-based Buffer Overflow Vulnerability	11/3/2021
CVE-2021-28550	Adobe	Acrobat and Reader	Adobe Acrobat and Reader Use-After-Free Vulnerability	11/3/2021
CVE-2018-4939	Adobe	ColdFusion	Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	11/3/2021
CVE-2018-15961	Adobe	ColdFusion	Adobe ColdFusion Unrestricted File Upload Vulnerability	11/3/2021
CVE-2018-4878	Adobe	Flash Player	Adobe Flash Player Use-After-Free Vulnerability	11/3/2021
CVE-2020-5735	Amcrest	Cameras and Network Video Recorder (NVR)	Amcrest Cameras and NVR Stack-based Buffer Overflow Vulnerability	11/3/2021
CVE-2019-2215	Android	Android Kernel	Android Kernel Use-After-Free Vulnerability	11/3/2021
CVE-2020-0041	Android	Android Kernel	Android Kernel Out-of-Bounds Write Vulnerability	11/3/2021
CVE-2020-0069	MediaTek	Multiple Chipsets	Mediatek Multiple Chipsets Insufficient Input Validation Vulnerability	11/3/2021

HCLSoftware

November 2023
BigFix Briefing Room

- Announcements & Upcoming Events
- Resources

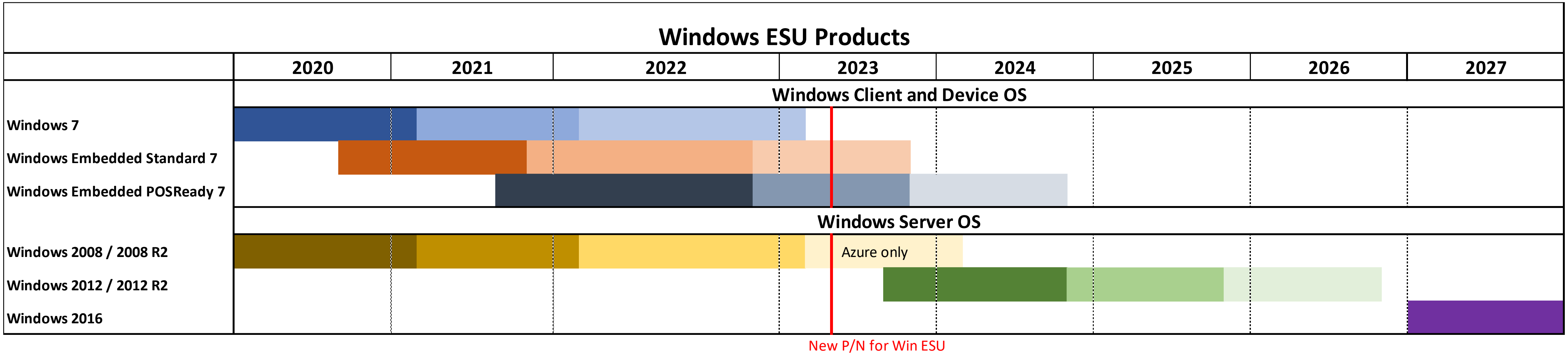
HCL BigFix

Windows Server 2012/2012 R2 End-of-Support

Windows Server 2012 and Windows Server 2012 R2 ends **TODAY**. These products will no longer receive security updates, non-security updates, bug fixes, technical support, or online technical content updates.

If you cannot upgrade to the next version, you will need to use Extended Security Updates (ESUs) for up to three years.

BigFix Support for Microsoft Windows Server 2012 ESU



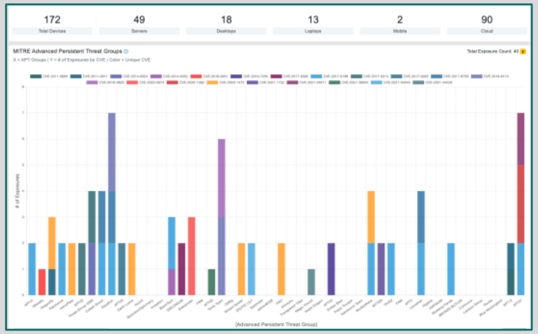
BigFix is offering Patch Add-On for Windows Server ESU

- Will work in conjunction with your Microsoft ESU agreement
- Will include BigFix content for Windows Server 2012/2012 R2, as well as Windows Server 2008.
- Contact your BigFix Tech Advisor for additional information or help through this process

#BigFixCanDoIt

BigFix CyberFOCUS

- Visualizations for CVE’s, KEV, and Threat groups.
- Extra Add-on component for detection of KEV items



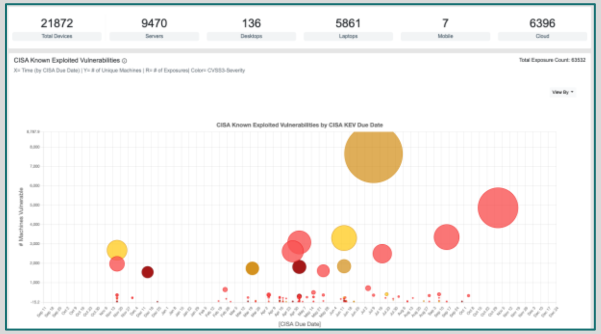
172	49	18	13	2	90
Total Devices	Servers	Desktops	Laptops	Mobile	Cloud

MITRE Advanced Persistent Threat Groups

X = APT Groups | Y = # of Exposures by CVE | Color = Unique CVE

Total Exposure Count: 40

Your Exposure to Known Attackers?



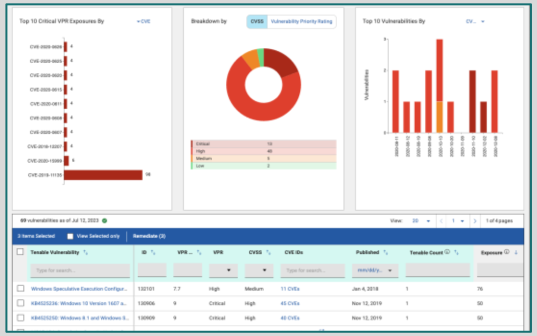
21872	9470	136	5861	7	6396
Total Devices	Servers	Desktops	Laptops	Mobile	Cloud

CISA Known Exploited Vulnerabilities

X= Time (by CISA Due Date) | Y= # of Unique Machines | R= # of Exposures| Color= CVSS3-Severity

Total Exposure Count: 63532

Your Exposure to Known Vulnerabilities?



Top 10 Critical VPR Exposures By
CVE
Breakdown by
CVSS
Vulnerability Priority Rating
Top 10 Vulnerabilities By
CV...
Vulnerabilities

Critical	13
High	40
Medium	5
Low	2

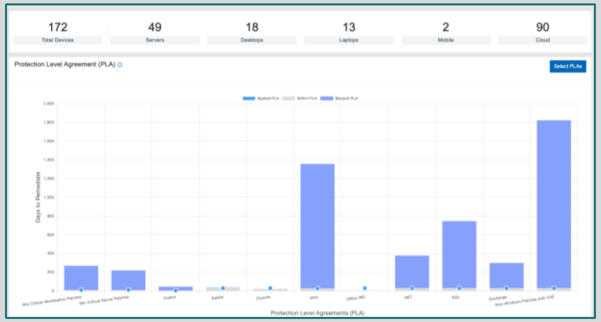
69 vulnerabilities as of Jul 12, 2023

View: 20 ‹ 1 › 1 of 4 pages

3 Items Selected ☐ View Selected only | Remediate (3)

☐	Tenable Vulnerability	ID	VPR ...	VPR	CVSS	CVE IDs	Published	Tenable Count	Exposure
☐	Windows Speculative Execution Configur...	132101	7.7	High	Medium	11 CVEs	Jan 4, 2018	1	76
☐	KB4525236: Windows 10 Version 1607 a...	130906	9	Critical	High	45 CVEs	Nov 12, 2019	1	50
☐	KB4525250: Windows 8.1 and Windows S...	130909	9	Critical	High	40 CVEs	Nov 12, 2019	1	50

Your Exposure to Discovered Vulnerabilities?



172	49	18	13	2	90
Total Devices	Servers	Desktops	Laptops	Mobile	Cloud

Protection Level Agreement (PLA)

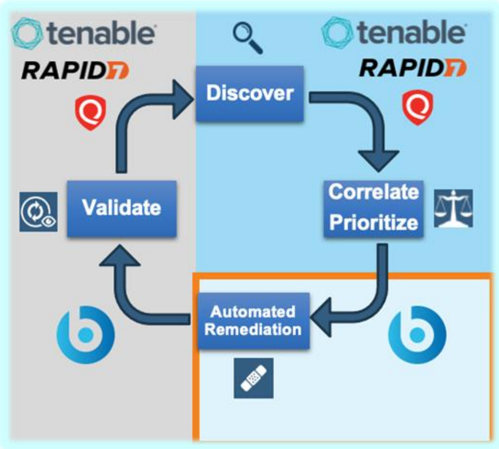
Select PLAs
Agreed PLA
Within PLA
Beyond PLA
Days to Remediate
Win Critical Workstation Patches
Win Critical Server Patches
Firefox
Adobe
Chrome
Java
Office 365
.NET
SQL
Exchange
Non-Windows Patches with CVE
Protection Level Agreements (PLA)

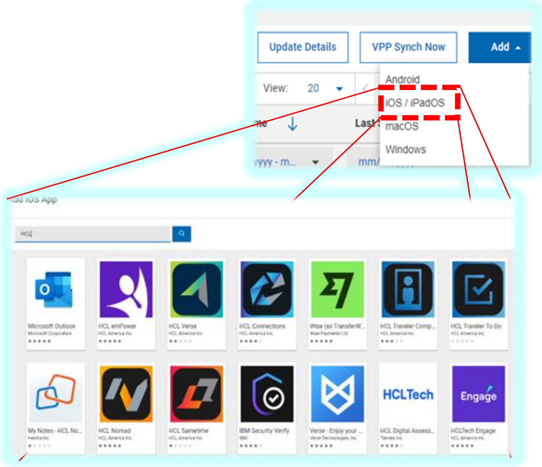
Proven Cyber Risk Reduction to C-Suite?

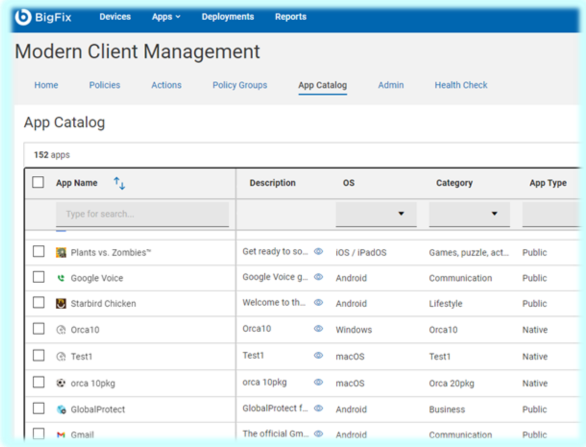
HCL BigFix | BigFix 11 is Here!

Why Upgrade?

- Expanded Remediation Integration for Rapid7 to coincide with Tenable & Qualys
  - Additional ability to import .csv's from other vulnerability scanning sources
- Support for Latest Mobile Management
- Support for SQL 2022
- Secure hardening of the BigFix Platform
  - Support for TLS 1.3
  - Upgraded OpenSSL v3
  - SHA-384 hashing
  - Recertified for FIPS 140-2







Modern Client Management

App Catalog

152 apps

App Name	Description	OS	Category	App Type
Plants vs. Zombies™	Get ready to so...	iOS / iPadOS	Games, puzzle, act...	Public
Google Voice	Google Voice g...	Android	Communication	Public
Starbird Chicken	Welcome to th...	Android	Lifestyle	Public
Orca10	Orca10	Windows	Orca10	Native
Test1	Test1	macOS	Test1	Native
orca 10pkg	orca 10pkg	macOS	Orca 20pkg	Native
GlobalProtect	GlobalProtect f...	Android	Business	Public
Gmail	The official Gm...	Android	Communication	Public

HCL BigFix | Upgrade Steps

Upgrade Checklist/Considerations

- ❑ Backups, Backups, Backups
  - ❑ Database backup after services have stopped at minimum
  - ❑ More comprehensive backup steps depending on your recovery requirements (VM snapshot for an easy button)
- ❑ Understand the Requirements – assumption of Upgrading to BigFix 11
  - ❑ Minimum OS & Database versions(Windows Server 2016/SQL Server 2014 & RHEL 8.1 /DB2 11.5)
  - ❑ Minimum BigFix version of 10.0.7
  - ❑ Enhanced Security enabled – Check KB0107321 for large environments
- ❑ Order is Key
  - ❑ Upgrade Server & Console, then Relays, then Agents
  - ❑ If relays are configured in a hierarchy, upgrade the top-level relays before the lower-level relays.
  - ❑ Respect the following rule: *server version >= relay version >= client version*

Patch Download Plugins Have Been Updated!

Benefit: Enhanced Security to Keep Your Credentials Safe!

- **Microsoft**
- **Adobe**
- **Red Hat**
- **Oracle**
- **More!**

This requires redeployment of the affected download plugins from the Manage Download Plugin Dashboard.

Learn more about this update on the BigFix Forum!

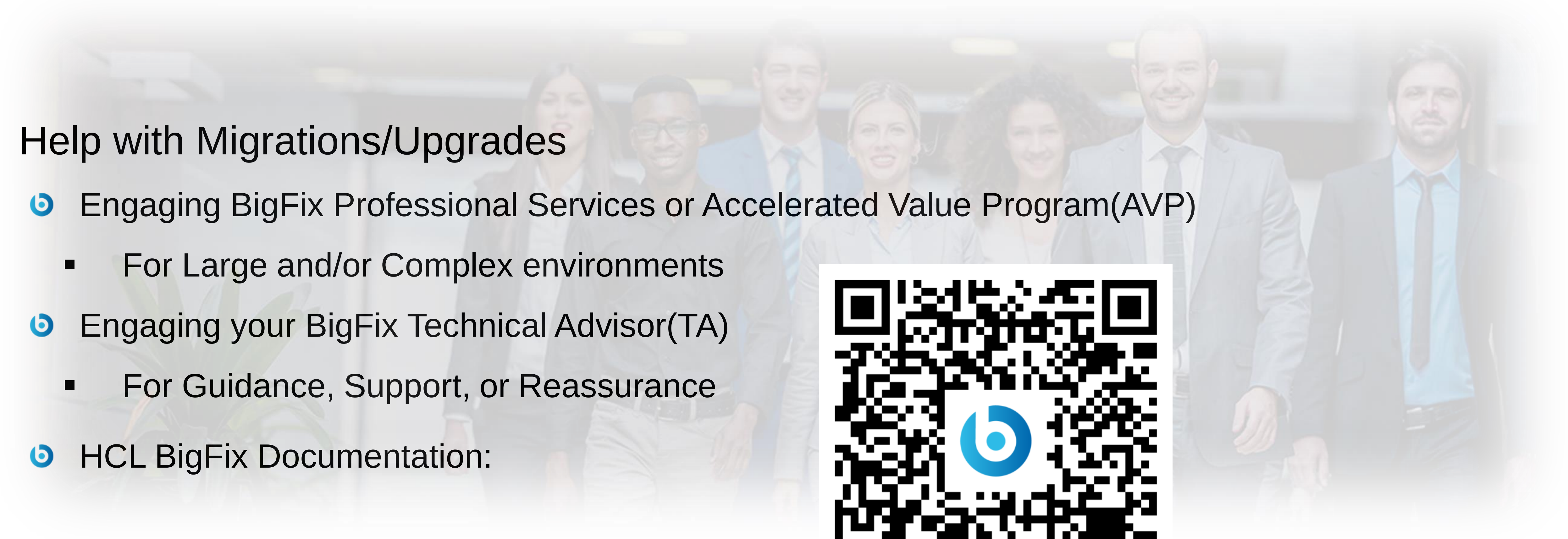
WebReports: Improved Print to .PDF!

Now print to pdf with the native Microsoft print to PDF driver in:

- **BigFix v11**
- **BigFix v10**
- **BigFix v9.523**

Learn more about this update on the BigFix Forum!

HCL BigFix | Additional Resources



Help with Migrations/Upgrades

- Engaging BigFix Professional Services or Accelerated Value Program(AVP)
  - For Large and/or Complex environments
- Engaging your BigFix Technical Advisor(TA)
  - For Guidance, Support, or Reassurance
- HCL BigFix Documentation:

On Your Mark.. Get BigFix Certified!

The Wait is OVER.
There’s a NEW shiny BigFix badge!

NEW!
HCLSoftware Certification for
BigFix Compliance 10 Administrator

HCLSoftware Certification for
BigFix Platform 10 Professional

HCLSoftware

Upcoming Events

In-Person Events

- East Coast US User Group

Webinars

Join us for these upcoming webinars and events…

December 2023 BigFix Briefing Room

December 13th 10 AM Pacific / 1 PM Eastern

January 2024 BigFix Briefing Room

January 10th 10 AM Pacific / 1 PM Eastern

HCLSoftware

Resources

Links for

- Documentation
- Mailing Lists
- Industry Media Resources

Mailing Lists

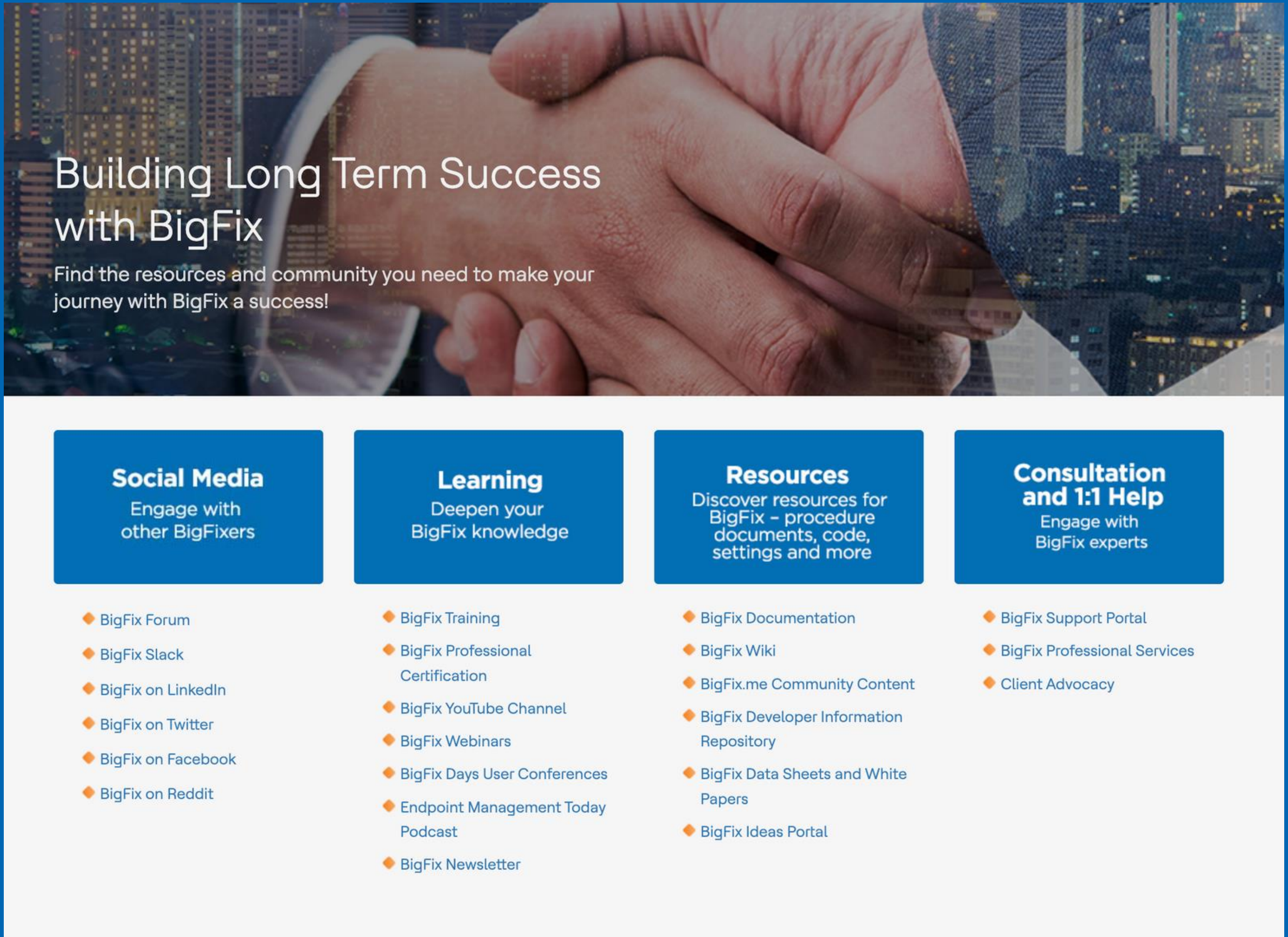
Be Among The First To Know!

- Receive Email announcements when new content is released
- View the archive to search for patches from previous announcements
- Announcements for various sites including:
  - BesAdmin-Announcements – Administrative and Windows Related Patching Information
  - RedHat-Announcements – RHEL patches
  - SUSE-Announcements – SUSE patches
  - HPUX-Announcements – HPUX patches
  - Oracle-Announcements – Oracle Linux patches

BigFix Email List

BigFix Administrative Announcements

BigFix Announcements Archives – current and previous announcements



Building Long Term Success with BigFix

Find the resources and community you need to make your journey with BigFix a success!

Social Media
Engage with other BigFixers

- BigFix Forum
- BigFix Slack
- BigFix on LinkedIn
- BigFix on Twitter
- BigFix on Facebook
- BigFix on Reddit

Learning
Deepen your BigFix knowledge

- BigFix Training
- BigFix Professional Certification
- BigFix YouTube Channel
- BigFix Webinars
- BigFix Days User Conferences
- Endpoint Management Today Podcast
- BigFix Newsletter

Resources
Discover resources for BigFix – procedure documents, code, settings and more

- BigFix Documentation
- BigFix Wiki
- BigFix.me Community Content
- BigFix Developer Information Repository
- BigFix Data Sheets and White Papers
- BigFix Ideas Portal

Consultation and 1:1 Help
Engage with BigFix experts

- BigFix Support Portal
- BigFix Professional Services
- Client Advocacy

Your one stop shop for all things BigFix related!

Thank You

HCLSoftware

hcltechsw.com