Your Microsoft Patch Tuesday Update, from team BigFix!

Rhonda Studnick Kaiser & Don Moss

Content overview

- October 2021 we got patches for 81 vulnerabilities.
- Of these, 3 are critical, 3 were previously disclosed and 1 is being exploited according to Microsoft.

Patch Tuesday October 2021

Microsoft today issued updates to plug more than 70 security holes in its **Windows** operating systems and other software, including one vulnerability that is already being exploited.

This month's Patch Tuesday also includes security fixes for the newly released **Windows 11 operating system

Apple has released iOS 15.0.2 and iPadOS 15.0.2 to fix a zero-day vulnerability (CVE-2021-30883) that is being leveraged in active attacks targeting iPhone and iPad users.

- Microsoft Summary Site

https://msrc.microsoft.com/update-guide/releaseNote/2021-Oct

Top Vulnerabilities

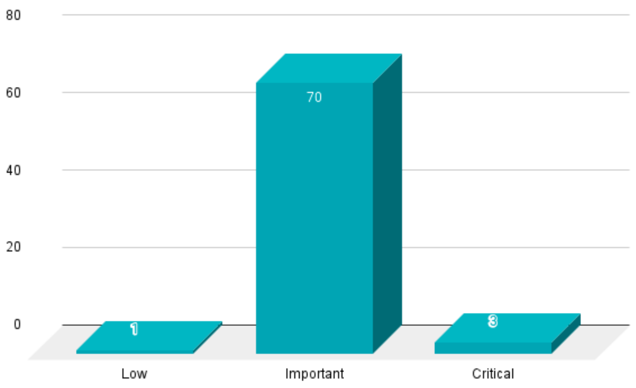
Microsoft October 2021 Patch Tuesday

71 vulnerabilities

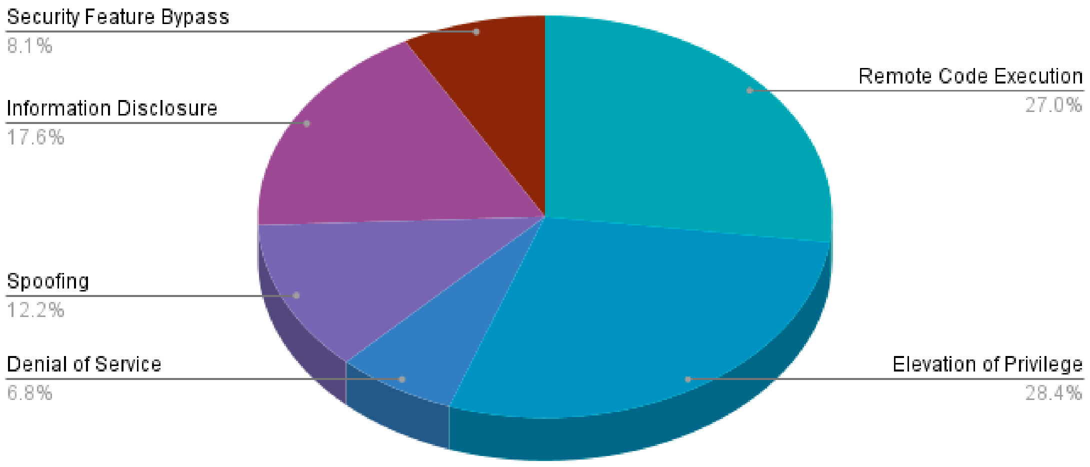
four zero-days

74 CVE’s

3 CRITICAL | 70 IMPORTANT | 0 MODERATE | 1 LOW



Count by Impact



Some techie stats:

Categorized Item Count :

Exchange Server :- 5

Windows :- 36

ESU :- 8

Microsoft Office :- 29

Microsoft Dynamics :- 5

Developer Tools :- 6

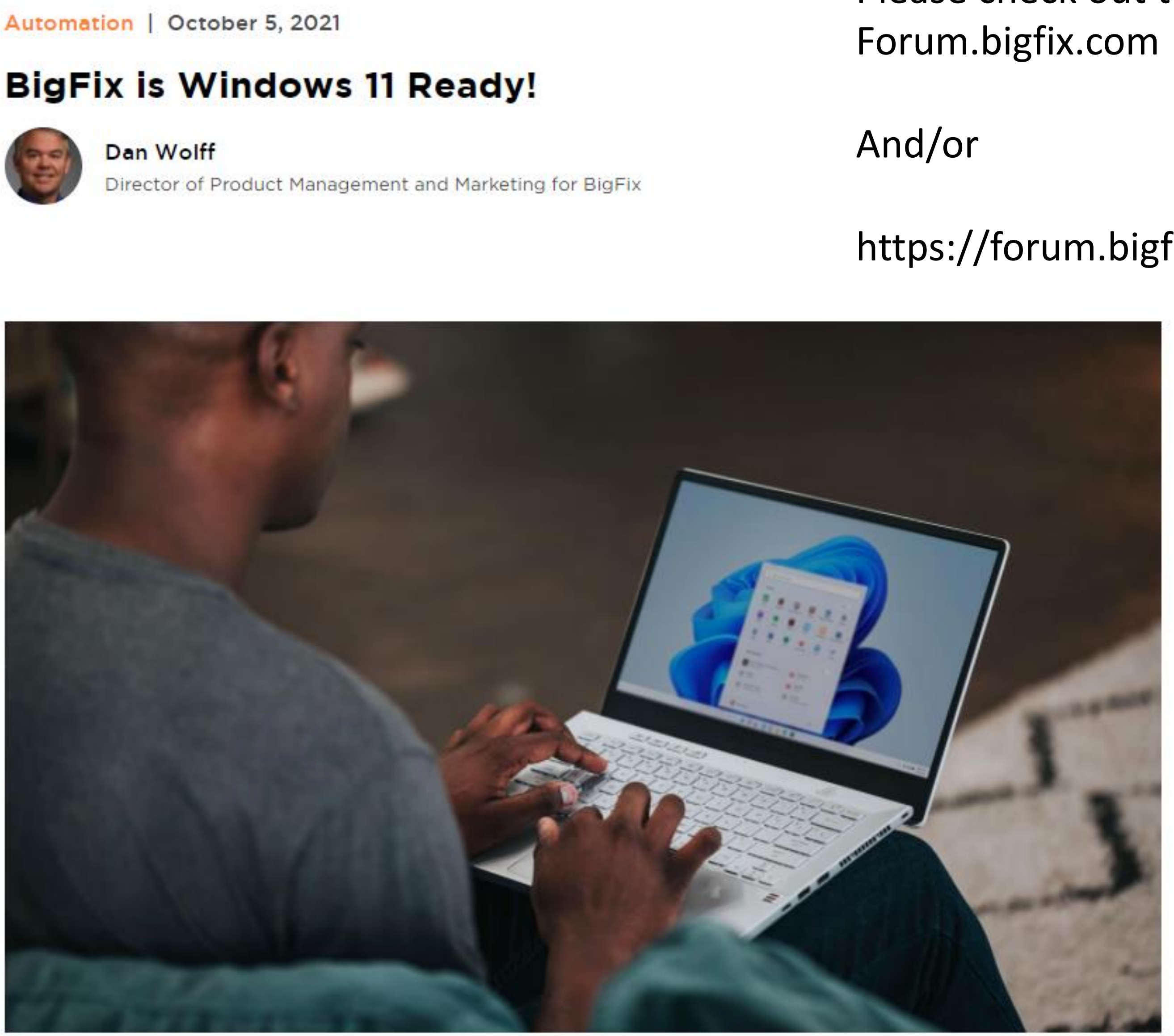
System Center :- 3

Browser :- 1

Apps :- 1

Exchange Server : 5
Windows : 36
ESU : 8
Microsoft Office : 29
Microsoft Dynamics : 5
Developer Tools : 6
System Center : 3
Browser : 1
Apps : 1

Categorized Item Count(Total) : 94
Individual Item Count : 94
TOTAL : 188



Automation | October 5, 2021

BigFix is Windows 11 Ready!

Dan Wolff

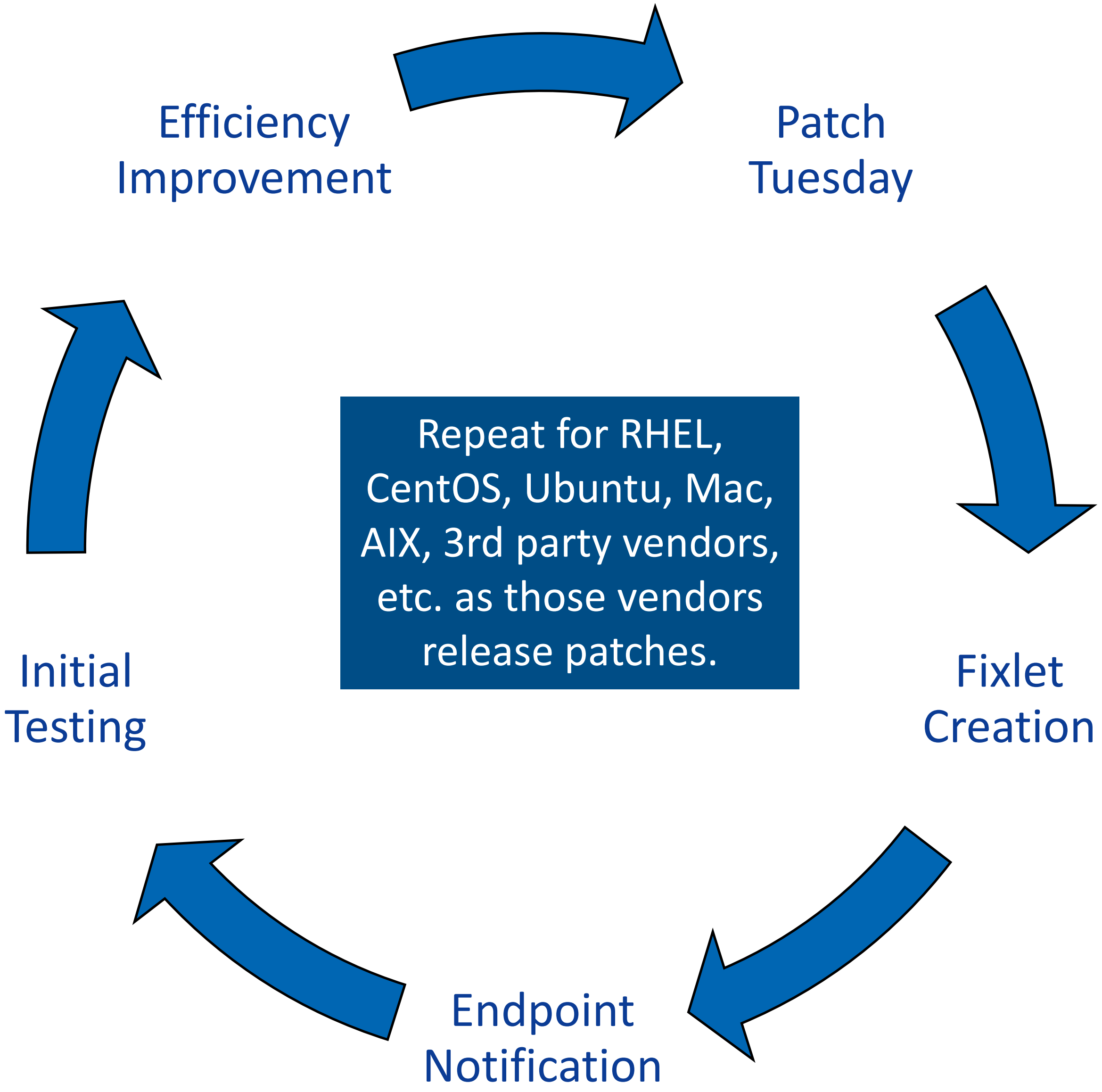
Director of Product Management and Marketing for BigFix

Please check out the BigFix forum on the latest info for Windows 11
Forum.bigfix.com

And/or

https://forum.bigfix.com/t/bigfix-windows-11/39300

BigFix Patch Release Process



Repeat for RHEL, CentOS, Ubuntu, Mac, AIX, 3rd party vendors, etc. as those vendors release patches.

BigFix Patching
BP’s & BKM’s

Various proactive tasks & options for delivering your patch payload in a smooth and efficient fashion!

Pre-Patch tips & prep

Additional thoughts and considerations!

- Do you have & use a test environment?
- Do you test 1 version of each OS in scope?
- Do you use a "batch mode" approach for deployments (which can include stagger)?
- Do you patch remote (internet based) devices? (more on next slide)
- Are you using the MS Patch Rollback wizard?

Copyright © 2019 HCL Technologies Limited | www.hcltech.com

Pre-Patch tips & prep

- Are you identifying target devices that need a reboot (aka pending restart)
- How long has it been since your systems were last rebooted (do you use a property that shows uptime)?
- Are you aware of your Cache Management tools (the size of these patches can get quite large)

See next size for example

Considerations for Work From Home computers, VPN load, etc

- _BESClient_Download_DirectRecovery = 1
- _BESClient_Download_Direct_Domainlist = *.adobe.com;*.apple.com;*.microsoft.com;*.bigfix.com;*.windowsupdate.com;*.ibm.com;*.google.com;*.mozilla.org

Disable evaluation of the PendingFileRenameOperations registry key
_BESClient_ActionManager_PendingRestartExclusions = :;

With _BESClient_WindowsOS_BypassPendingRestartRelevance enabled, the fixlet view will not show remediated until the endpoint has restarted and completely applied the patch.

HCL SOFTWARE
Copyright © 2019 HCL Technologies Limited | www.hcltech.com

Pre-Patch tips & prep

Deploy patches in three phases to minimize risk of patches causing problems in your entire environment.

- Pilot group – A small number of endpoints that represent all operating systems and applications in your environment. Up to a few hundred systems. Restart these systems more aggressively to ensure a timely test.

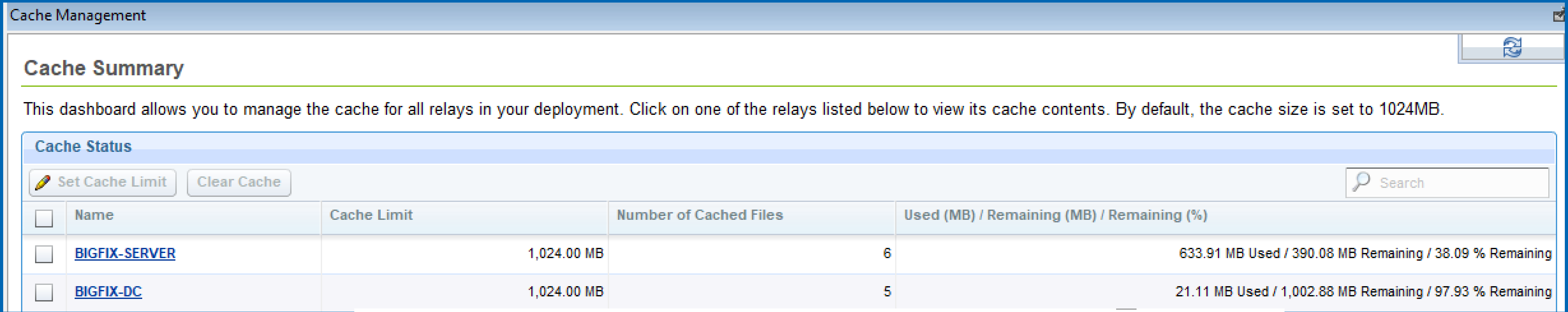
- Test scale group – larger number of systems, these can be defined randomly with the Mod relevance inspector. Using the following relevance in your action script will target 5% of all computers.
computer id mod 20 = 1

- Full deployment.

HCL SOFTWARE

Pre-Patch tips & prep

- Do you have patches that have been deploying successfully and all of the sudden you see “pending downloads” in the console for systems in certain locations?
- Might be a cache constraint issue. How much cache do you have allocated on your relays? It’s easy to check.

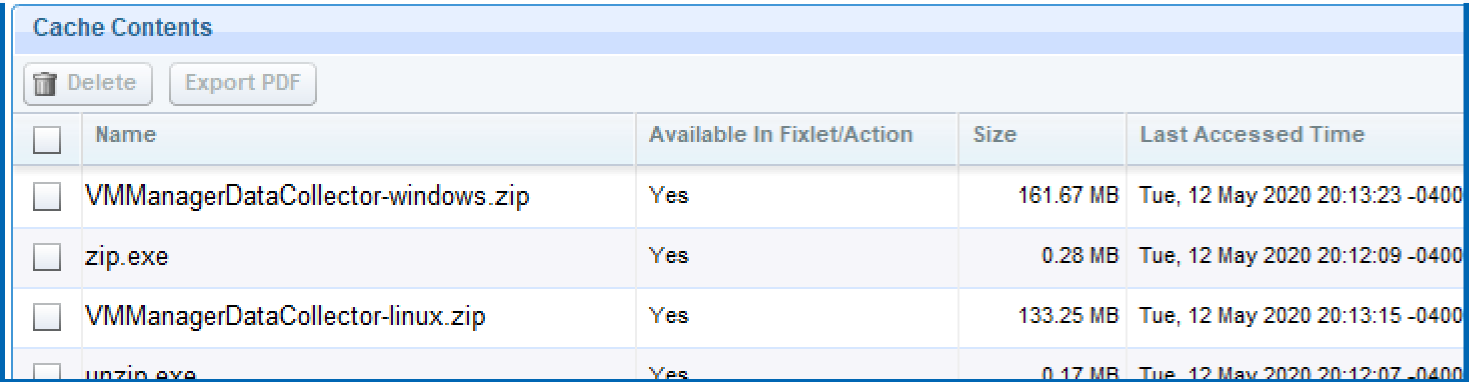

Cache Management

Cache Summary

This dashboard allows you to manage the cache for all relays in your deployment. Click on one of the relays listed below to view its cache contents. By default, the cache size is set to 1024MB.

Cache Status

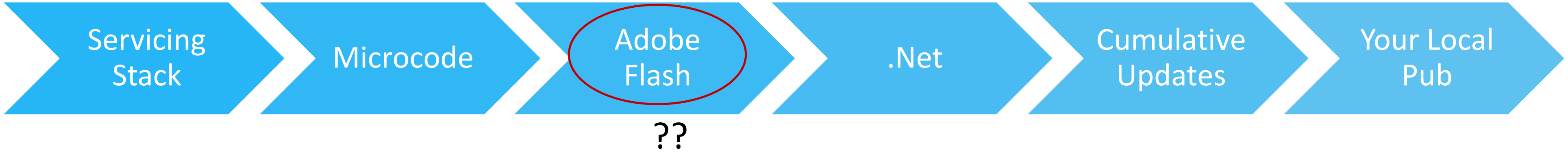
□	Name	Cache Limit	Number of Cached Files	Used (MB) / Remaining (MB) / Remaining (%)
□	BIGFIX-SERVER	1,024.00 MB	6	633.91 MB Used / 390.08 MB Remaining / 38.09 % Remaining
□	BIGFIX-DC	1,024.00 MB	5	21.11 MB Used / 1,002.88 MB Remaining / 97.93 % Remaining


Cache Contents

□	Name	Available In Fixlet/Action	Size	Last Accessed Time
□	VMManagerDataCollector-windows.zip	Yes	161.67 MB	Tue, 12 May 2020 20:13:23 -0400
□	zip.exe	Yes	0.28 MB	Tue, 12 May 2020 20:12:09 -0400
□	VMManagerDataCollector-linux.zip	Yes	133.25 MB	Tue, 12 May 2020 20:13:15 -0400
□	unzip.exe	Yes	0.17 MB	Tue, 12 May 2020 20:12:07 -0400

Don’t forget your best practices

Service stack updates before Cumulative updates!



- Don’t create baselines in the MasterAction site.
- Make use of custom filters to short-cut your search time
- Restart before and after deployment, or monitor the ‘restart needed’ fixlets, or have a report automatically sent to you if there are machines still pending restarts a few days before your next patch deployment cycle.
- Remember to sync baselines - **Depends on your patching process**
- Pre cache binaries on your Relays to speed up patching
- Pre cache locally an option as well
- Do you need a Relay at all? – peer nesting ☺

Suggested Baseline BP's-BKM

Just as info, we use baselines in excess of 100 components with no ill effects but we have keep to below 200 and we never have our baselines in the master action site.

Limit number of components to 100 (I've seen more - but needs to be managed)

Use custom sites to store your baselines (keep them out of the Master Action Site)

Do not blindly select relevant fixlets (selecting all relevant fixlets is a recipe for disaster)

Do not add administrative fixlets/tasks to your patching baseline (for example: upgrading your BigFix client); keep the intent of your patching baseline to patching only

Read the description of the patching fixlets for important critical notes before deciding to deploy them

Avoid including service pack level updates or large updates to your critical/important patching baselines; action on them separately

Do not add patching fixlets which contain the words "CORRUPT PATCH" in their Name to your baseline (

Do not add patching fixlets which contain the word "Superseded in their Name to your baseline

Ensure each component has an action selected

Maintain and re-synchronize your baselines over time

Retire / delete baselines that are no longer needed

Make sure to use the Baseline Sync dashboard to keep your baselines current & updated!

Remember - instead of using baselines, there is the Patch Policy feature in WebUI which can negate the need for patch baselines.

Automate Patching

Via the BigFix WebUI!

The BigFix WebUI was initially designed as a web enabled console ideal for "Junior" operators in BigFix that didn't need the breadth and function of the installed BigFix console.

Over time we added new features not found in the installed BigFix console such as:

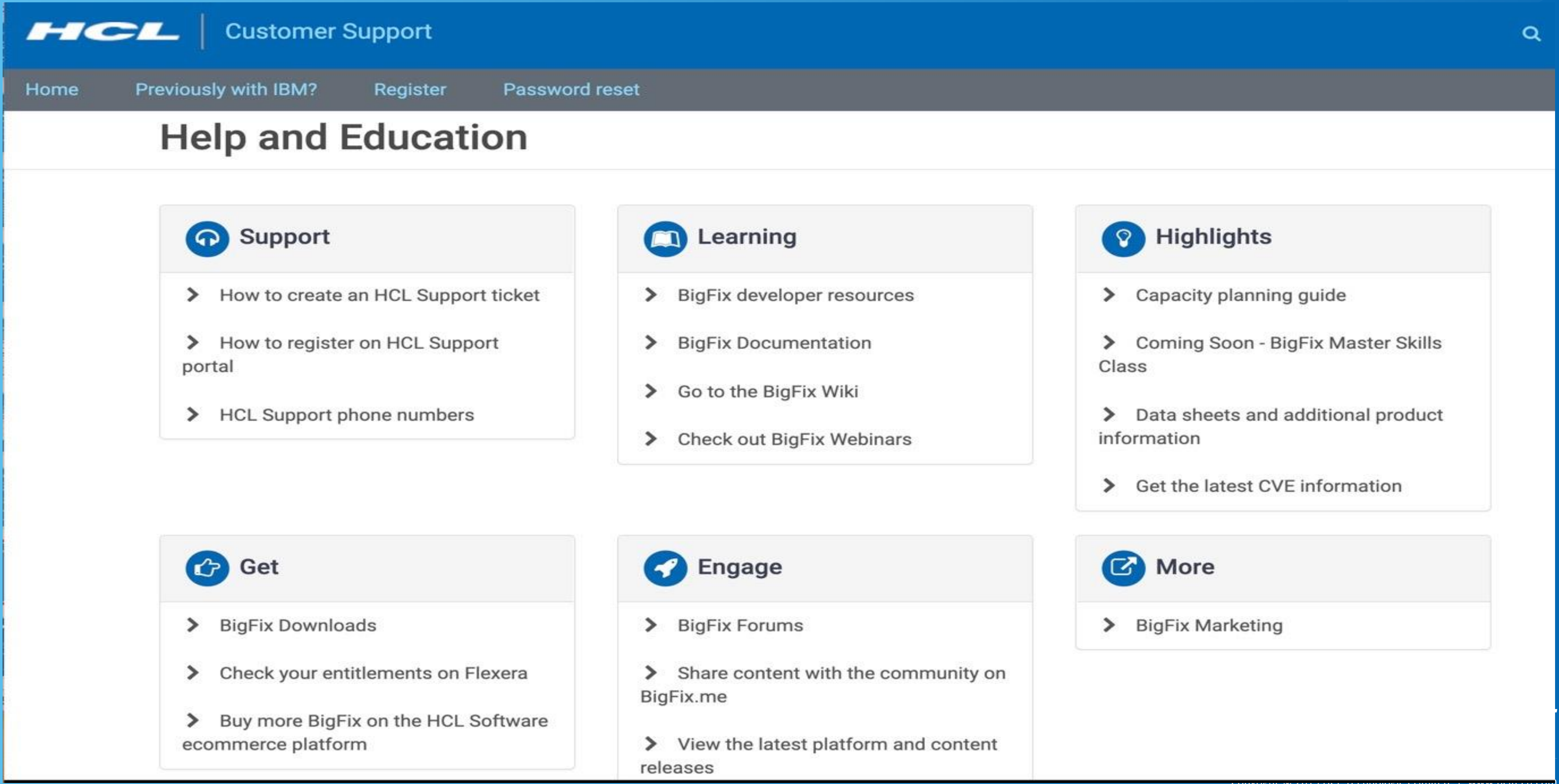
- Icon support for software distribution via the BigFix Self Service Application
- Query for rapid interrogation of endpoints
- Mac and Win10 Profile management
- Executive Dashboards/Reporting
- …And Patch Policies for automated patching:

  https://support.bigfix.com -> Events -> Webinars

  - November Microsoft Patch Content Review

  - Master Your Endpoints

BigFix Resources – support.bigfix.com



Home | Previously with IBM? | Register | Password reset

Help and Education

Support

- How to create an HCL Support ticket
- How to register on HCL Support portal
- HCL Support phone numbers

Learning

- BigFix developer resources
- BigFix Documentation
- Go to the BigFix Wiki
- Check out BigFix Webinars

Highlights

- Capacity planning guide
- Coming Soon - BigFix Master Skills Class
- Data sheets and additional product information
- Get the latest CVE information

Get

- BigFix Downloads
- Check your entitlements on Flexera
- Buy more BigFix on the HCL Software ecommerce platform

Engage

- BigFix Forums
- Share content with the community on BigFix.me
- View the latest platform and content releases

More

- BigFix Marketing

HCL

Thank you & Happy Patching!

Relationship™

BEYOND THE CONTRACT

$8.4 BILLION ENTERPRISE | 132,000 IDEAPRENEURS | 44 COUNTRIES

▶ WATCH THE FILM