



Qualys Patch Management

Release Notes

Version 1.5.2

August 16, 2021 (updated September 11, 2021)

Here's what's new in Patch Management 1.5.2!

[View Missing Patches for Linux Assets](#)

[Update to the Limit on Adding Assets and Asset Tags to a Single Job](#)

[New OS support](#)

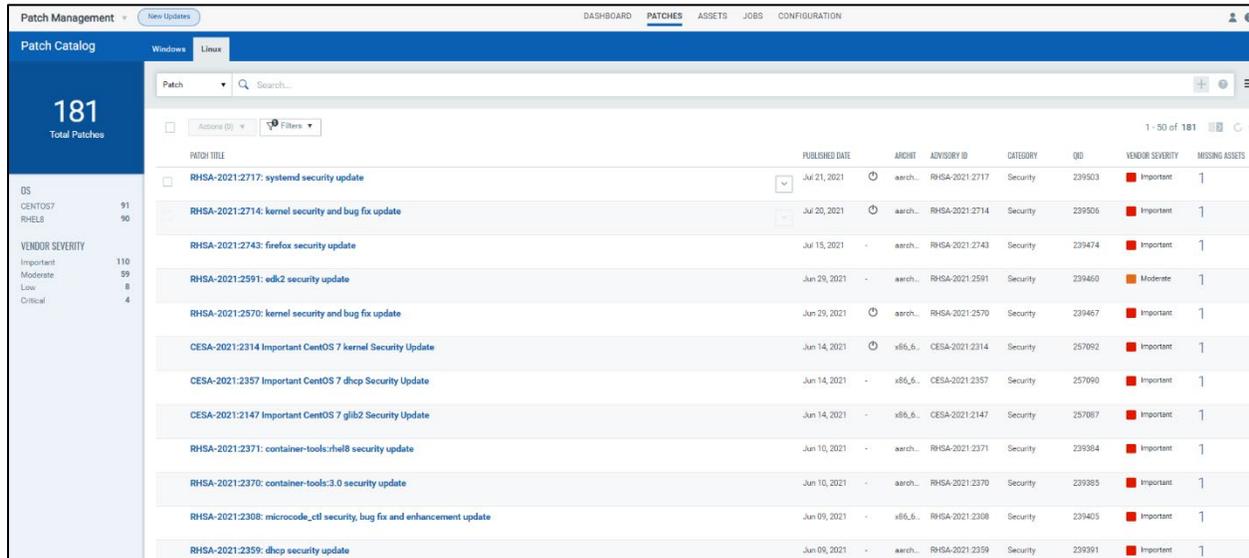
[Create QQL-based Jobs to Remediate Windows Vulnerabilities](#)

[Patch Linux assets from the VMDR App](#)

Qualys 1.5.2 brings you more improvements and updates! [Learn more](#)

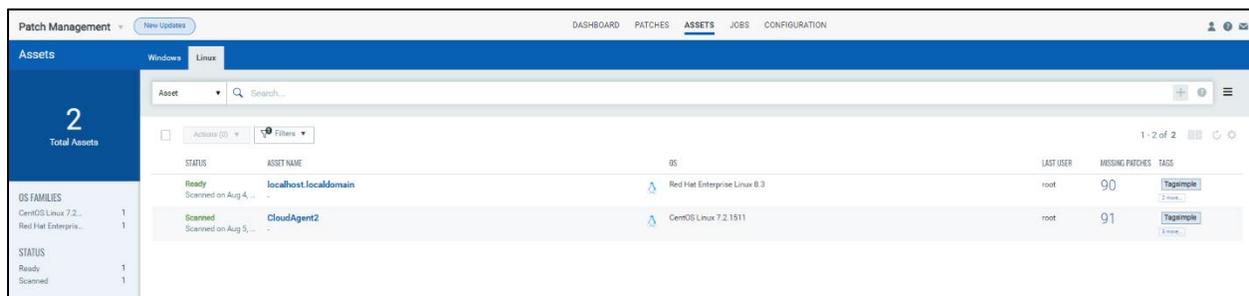
View Missing Patches for Linux Assets

The patches listed in the Patch Management patch catalog are missing on your hosts, which were detected using the vulnerability scan. The vulnerability scan provides details about detected vulnerabilities. These detected vulnerabilities can be mapped to missing patches respectively on the Linux agent.



Patch Title	Published Date	Arch	Advisory ID	Category	OID	Vendor Severity	Missing Assets
RHSA-2021:2717: systemd security update	Jul 21, 2021	aarch...	RHSA-2021:2717	Security	239503	Important	1
RHSA-2021:2714: kernel security and bug fix update	Jul 20, 2021	aarch...	RHSA-2021:2714	Security	239506	Important	1
RHSA-2021:2743: firefox security update	Jul 15, 2021	aarch...	RHSA-2021:2743	Security	239474	Important	1
RHSA-2021:2591: edk2 security update	Jun 29, 2021	aarch...	RHSA-2021:2591	Security	239460	Moderate	1
RHSA-2021:2570: kernel security and bug fix update	Jun 29, 2021	aarch...	RHSA-2021:2570	Security	239467	Important	1
CESA-2021:2314 Important CentOS 7 kernel Security Update	Jun 14, 2021	x86_64	CESA-2021:2314	Security	257092	Important	1
CESA-2021:2357 Important CentOS 7 dhcp Security Update	Jun 14, 2021	x86_64	CESA-2021:2357	Security	257090	Important	1
CESA-2021:2147 Important CentOS 7 glib2 Security Update	Jun 14, 2021	x86_64	CESA-2021:2147	Security	257087	Important	1
RHSA-2021:2371: container-tools:rhel8 security update	Jun 10, 2021	aarch...	RHSA-2021:2371	Security	239384	Important	1
RHSA-2021:2370: container-tools:3.0 security update	Jun 10, 2021	aarch...	RHSA-2021:2370	Security	239385	Important	1
RHSA-2021:2308: microcode_ctl security, bug fix and enhancement update	Jun 09, 2021	x86_64	RHSA-2021:2308	Security	239405	Important	1
RHSA-2021:2359: dhcp security update	Jun 09, 2021	aarch...	RHSA-2021:2359	Security	239391	Important	1

Alternatively, you can go to the Assets tab to view missing patches on assets. Once a deployment job on the Linux asset is executed, the missing patches will be updated when a subsequent vulnerability scan is completed.



Status	Asset Name	OS	Last User	Missing Patches	Tags
Ready Scanned on Aug 4, ...	localhost.localdomain	Red Hat Enterprise Linux 8.3	root	90	Example Linux
Scanned Scanned on Aug 5, ...	CloudAgent2	CentOS Linux 7.2.1511	root	91	Example Linux

Update to the Limit on Adding Assets and Asset Tags to a Single Job

For a single job, you can include and exclude a maximum of 50 assets and 50 asset tags. If you want to include more than 50 assets, we recommend that you use asset tags. If you want to include more than 50 asset tags, we recommend creating a tag hierarchy. Add only parent tags to the job, and our system will automatically include its child tags even if the child tags are more than 50. Refer to the Manage Asset Tags topic in the Qualys CyberSecurity Asset Management (CSAM) to learn more about tags.

These limits are applicable for Windows and Linux jobs. If the existing jobs contain more than 50 assets or asset tags, the jobs are not impacted. However, if you edit an existing job, the new limits are applicable.

New OS support

You can now patch Linux assets with the following operating systems:

- RHEL 8
- CentOS 7
- CentOS 6

Note: You must update the Cloud Agent version to 4.6 to use this functionality.

Create QQL-based Jobs to Remediate Windows Vulnerabilities

You now create QQL-based deployment jobs using specific vulnerabilities attributes for Windows assets. This allows you to automate deployment jobs to remediate specific vulnerabilities regularly.

← Create: Windows Deployment Job

STEPS 3/7

- 1 Basic Information
- 2 Select Assets
- 3 Select Patches
- 4 Schedule
- 5 Options
- 6 Job Access
- 7 Confirmation

Select Patches

Choose the patches you want to install for the selected assets or create a query for the job.

Select Patches Create a Query for Patches

Vulnerability

Patch performance, only missing and non-superseded patches that match the QQL criteria will be added to the job.

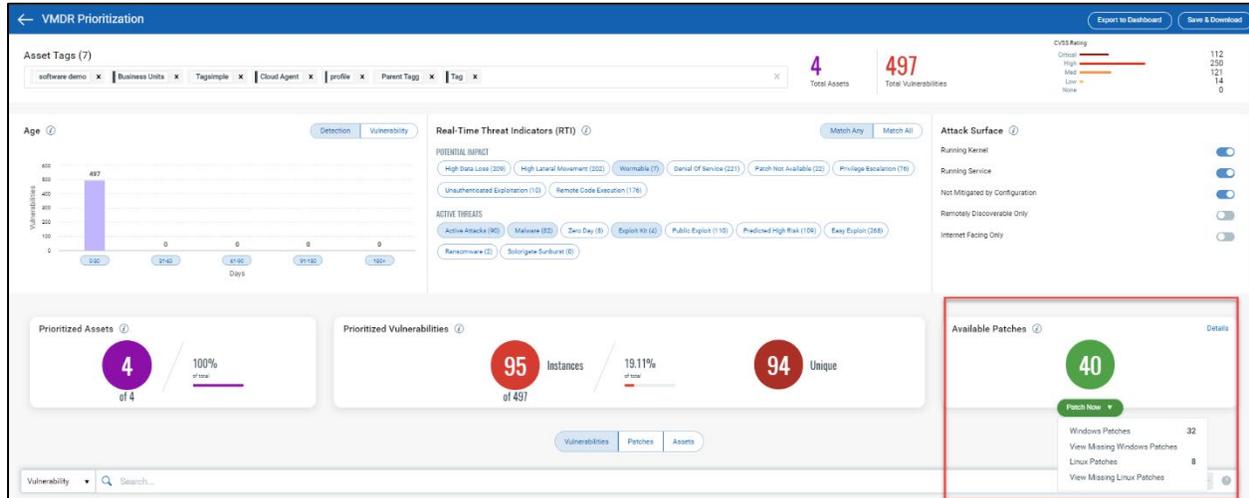
Vulnerability

Cancel Previous Next

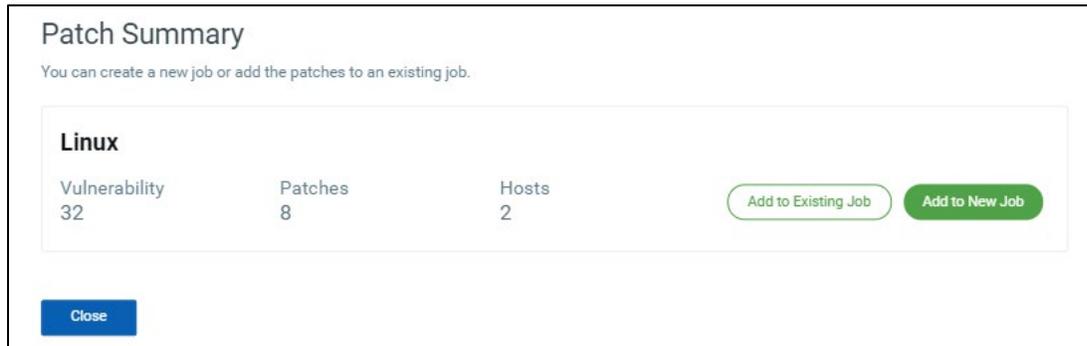
Note: You must have a subscription to the Patch Management app to remediate the Linux vulnerabilities.

Patch Linux assets from the VMDR App

You can now remediate Linux vulnerabilities using the Patch Now option in a Prioritization report. You can also view patches that are missing on Linux assets.



You can add the available Linux patches to an existing job or create a new job to remediate the vulnerabilities.



Note: You must have a subscription to the Patch Management app to remediate the Linux vulnerabilities.

Issues Addressed

- We fixed an issue where the stale assets were not removed from the Patch Management UI.
- We fixed an issue where if you added the assets to a new job from the **Assets** tab, the assets took too long time to load on the **Job Configuration** tab.
- We fixed an issue where the isSuperseded filter was not honored on the **Assets** tab for patches search criteria.
- We fixed an issue where the vulnerability count in the Prioritized Product report included all vulnerabilities instead of only the unique vulnerabilities.