

# Qualys Patch Management

## Release Notes

Version 2.4

August 03, 2023 (Last Updated on August 18, 2023)

### What's New

Here's what's new in Patch Management 2.4!

[Add Custom Repository URLs and Edit Custom Repository URLs Pages Enhancements](#)

[Prioritized Products Tab Enhancements](#)

[Enhanced Visibility for Windows Patch Failure](#)

[Support for Linux Patch Report Download](#)

[RHEL9 and Oracle Linux 9 Patching Support](#)

[Rocky Linux 8, 9 and Alma Linux 8, 9 Support](#)

[DST Honored for Scheduled Patch Jobs](#)

Qualys 2.4 brings you more improvements and updates! [Learn more](#)

## Add Custom Repository URLs and Edit Custom Repository URLs Pages Enhancements

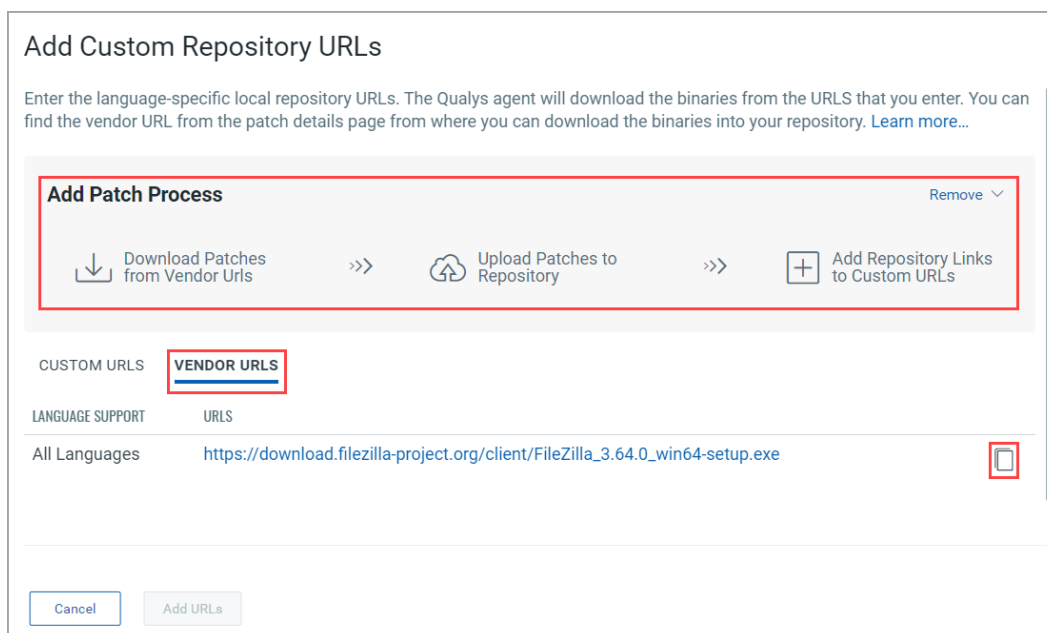
The “Add Custom Repository URLs” and “Edit Custom Repository URLs” pages are enhanced to include the **Vendor URL** tab and the **Add Patch Process** representation.

**Note:** You see these pages when you enable the “AcquireFromVendor” type of Windows patches for adding to existing or new Windows deployment jobs. For more information, see [Enabling Vendor-Acquired Patch](#).

- **Vendor URLs** tab: With the introduction of this tab, you are no longer required to go to the “Patch Details” page to know the Vendor URL. Instead, click the **Vendor URLs** tab to see the

vendor URL. Click the **Copy**  icon to copy the Vendor URL and complete further steps.




- **Add Patch Process** representation: The intuitive representation of the **Add Patch Process** provides guidance on the same screen. You can hide the **Add Patch Process** representation by clicking **Remove**.




**Add Custom Repository URLs**

Enter the language-specific local repository URLs. The Qualys agent will download the binaries from the URLs that you enter. You can find the vendor URL from the patch details page from where you can download the binaries into your repository. [Learn more...](#)

**Add Patch Process** Remove ▾

 Download Patches from Vendor Urls >>  Upload Patches to Repository >>  Add Repository Links to Custom URLs

| CUSTOM URLS      | VENDOR URLS   |
|------------------|---|
| LANGUAGE SUPPORT | URLS  |
| All Languages    | <a href="https://download.filezilla-project.org/client/FileZilla_3.64.0_win64-setup.exe">https://download.filezilla-project.org/client/FileZilla_3.64.0_win64-setup.exe</a>  |

Cancel Add URLs

## Prioritized Products Tab Enhancements

The **Risk Reduction Recommendation** tab is introduced under the **Prioritized Products** tab. When you click this tab, you can see a maximum of 50 entries of recommended, latest patches based on the top high and critical QID count. You can achieve a risk reduction on your Windows assets by creating jobs using these suggested latest patches. For more information, see [Prioritizing Product Vulnerabilities for Windows Assets](#).

Patch Management

New Updates

DASHBOARD

PRIORITIZED PRODUCTS

PATCHES

ASSETS

JOB

CONFIGURATION

<

Enhanced Visibility for Windows Patch Failure

New exit codes are introduced as part of error codes for Windows patch failure. As a result, you get visibility into the root cause of the patch failure and the possible solution to fix the issue.

When you click the **Exit Code** from the Error Codes section of the 'Failure Details' popup, you can see the newly introduced “Exit Code” popup, wherein you can see the possible root cause and possible solution to fix the issue. For more information, see [Viewing Windows Patch Failure Error Code Details](#) and [Patch-Specific Failure Reason Codes for Windows](#).

Failure Details

Refer to the failure reason and error codes for more details.

Reason for Failure

FileHashValidationFailed: The vendor patch file failed the hash validation.

Error Codes

HTTP Status

500

OS Status

5

Exit Code

1642

Note: To know more about the error codes, [click here](#).

Close

Exit Code

Abstract

The Windows Installer service couldn't install the upgrade patch because either the program to be upgraded might be missing or the upgrade patch might update a different version of the program.

Possible Root Cause

The version of the program targeted in the patch differs from the one on the agent machine. It might happen when an upgrade in the application is done in any other way before the actual patch installation.

Possible Solution


The issue will be resolved by selecting the correct patch that supports the application version on the endpoint. But if the targeted application is already updated, you can ignore this message.

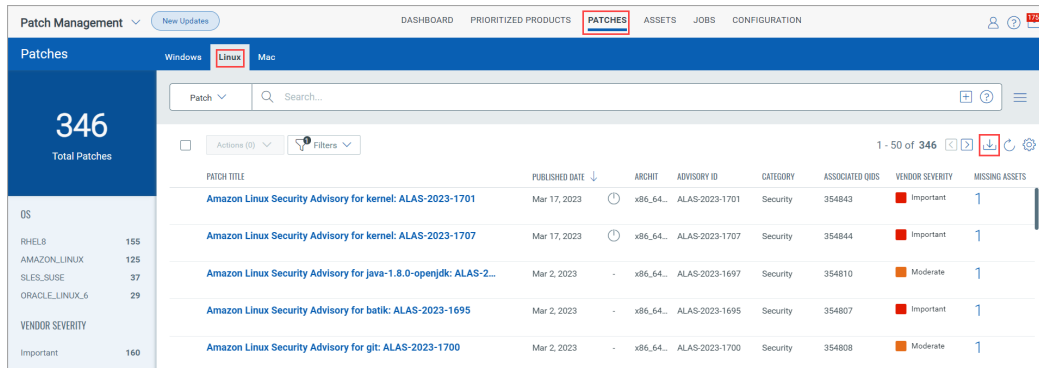
Learn More

Close

## Support for Linux Patch Report Download

You can download the detailed patch data for Linux assets from the **Patches** and **Assets** tabs. Before this release, this support was available for only Windows assets.

As shown in the following screen capture, click the **Download**  icon to download the patch data report for Linux. For more information, see [Generating Patch Reports for Windows and Linux Assets](#).

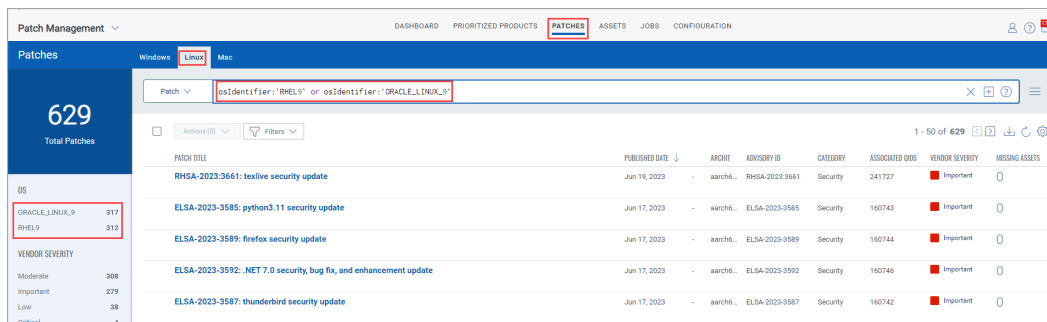


The screenshot shows the Patch Management interface with the **Patches** tab selected. The left sidebar shows a total of 346 patches. The main table lists patches for Linux, including Amazon Linux Security Advisories for kernel, java, batik, and git. A download icon is visible in the top right of the table.

| Patch Title  | Published Date | Arch      | Advisory ID    | Category | Associated QIDs | Vendor Severity | Missing Assets |
|--|----------------|-----------|----------------|----------|-----------------|-----------------|----------------|
| Amazon Linux Security Advisory for kernel: ALAS-2023-1701        | Mar 17, 2023   | x86_64... | ALAS-2023-1701 | Security | 354843          | Important       | 1              |
| Amazon Linux Security Advisory for kernel: ALAS-2023-1707        | Mar 17, 2023   | x86_64... | ALAS-2023-1707 | Security | 354844          | Important       | 1              |
| Amazon Linux Security Advisory for java-1.8.0-openjdk: ALAS-2... | Mar 2, 2023    | x86_64... | ALAS-2023-1697 | Security | 354810          | Moderate        | 1              |
| Amazon Linux Security Advisory for batik: ALAS-2023-1695         | Mar 2, 2023    | x86_64... | ALAS-2023-1695 | Security | 354807          | Important       | 1              |
| Amazon Linux Security Advisory for git: ALAS-2023-1700           | Mar 2, 2023    | x86_64... | ALAS-2023-1700 | Security | 354808          | Moderate        | 1              |

## RHEL9 and Oracle Linux 9 Patching Support

You can now patch the RHEL9.x (RHEL 9.0, RHEL 9.1, RHEL 9.2) and Oracle Linux 9 patches for the Linux platform.

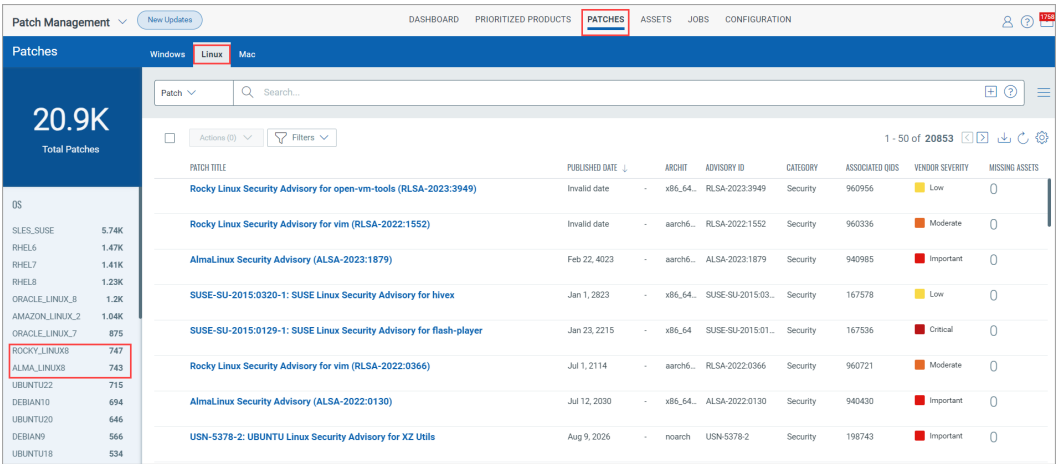


The screenshot shows the Patch Management interface with the **Patches** tab selected. The left sidebar shows a total of 629 patches. The search bar is set to `osIdentifier:'RHEL9' or osIdentifier:'ORACLE.LINUX.9'`. The main table lists patches for RHEL9 and Oracle Linux 9, including RHSA-2023-3661, ELSA-2023-3585, ELSA-2023-3589, ELSA-2023-3592, and ELSA-2023-3587. A download icon is visible in the top right of the table.

| Patch Title  | Published Date | Arch       | Advisory ID    | Category | Associated QIDs | Vendor Severity | Missing Assets |
|--|----------------|------------|----------------|----------|-----------------|-----------------|----------------|
| RHSA-2023-3661: texlive security update                            | Jun 19, 2023   | aarch64... | RHSA-2023-3661 | Security | 241727          | Important       | 0              |
| ELSA-2023-3585: python3.11 security update                         | Jun 17, 2023   | aarch64... | ELSA-2023-3585 | Security | 160743          | Important       | 0              |
| ELSA-2023-3589: firefox security update                            | Jun 17, 2023   | aarch64... | ELSA-2023-3589 | Security | 160744          | Important       | 0              |
| ELSA-2023-3592: .NET 7.0 security, bug fix, and enhancement update | Jun 17, 2023   | aarch64... | ELSA-2023-3592 | Security | 160746          | Important       | 0              |
| ELSA-2023-3587: thunderbird security update                        | Jun 17, 2023   | aarch64... | ELSA-2023-3587 | Security | 160742          | Important       | 0              |

# Rocky Linux 8, 9 and Alma Linux 8, 9 Support

We added support for Linux 8, 9 and Alma Linux 8, 9.



## DST Honored for Scheduled Patch Jobs

DST is honored for all types of scheduled new patch jobs. To honor the DST for existing jobs that are already enabled, you must disable them first and enable them again.

## Issues Addressed

- We fixed the Report Generation failure issue in the scenarios where the useruuid used for report generation doesn't belong to the customeruuid.
- We fixed the pre-action and post-action script execution failure issue for Linux assets.
- We fixed the issue where the discrepancy was observed in the case of the missing patches shown on the Patch Management UI and the downloaded report for the same assets.
- We fixed an issue where an incorrect recurring day was assigned in the weekly job despite selecting the correct recurring day.
- We fixed the job schedule issue for Patch Tuesday jobs.
- We enhanced the [Patch Management license consumption representation](#) on the UI for the License consumption exceeds your license limit scenario to provide more clarity.
- We added the \*.gvt1.com domain to the allowlist documentation to avoid the HTTP 407 error scenario observed for one of the patch URLs with the \*.gvt1.com domain.