Software Vulnerability Manager (Cloud Edition) Release Notes

May 2023 - Update 2

Introduction

Flexera's Software Vulnerability Manager is a software vulnerability and patch management solution that facilitates a customized patch management process. It combines vulnerability and threat intelligence, end point assessment, and patch creation and publishing enable an informed and rapid patch management.

Software Vulnerability Manager can assess software vulnerabilities for both Microsoft and non-Microsoft (third-party) product vulnerabilities covering Microsoft Windows, macOS, and Red Hat Enterprise Linux. The results of this assessment are connected to our vulnerability and threat intelligence to allow for effective prioritization. Finally, third party patches may be created and published to remediate endpoints using Microsoft® WSUS (often in conjunction with System Center Configuration Manager), via Microsoft® Intune, VMware® Workspace One, or BigFix.

New Features and Enhancements

Software Vulnerability Manager (Cloud Edition) includes the following new features and enhancements:

- Patch Publisher Enhancements
- Software Vulnerability Manager User Interface Enhancements
- WSUS Management Tool Improvements
- Reference: Latest Binary Versions

Note • *To see the following new features and enhancements in your Software Vulnerability Manager (Cloud Edition) interface, you must refresh your browser's cache (press Ctrl+F5).*

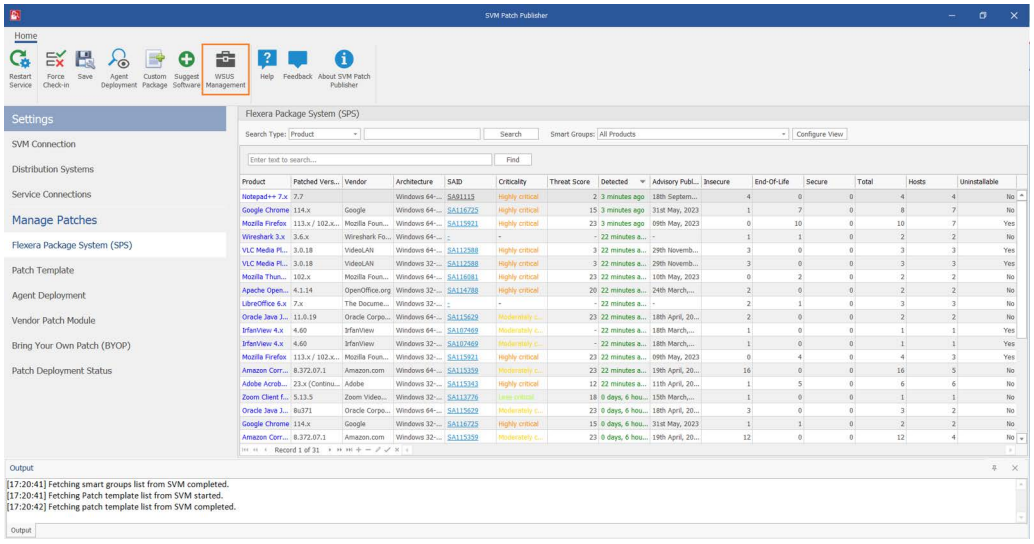
Patch Publisher Enhancements

The following improvements have been added to the SVM Patch Publisher.

- WSUS Management Tool Integration with SVM Patch Publisher
- Support for SSO Authentication in SVM Connection
- Hyperlinks in Advisory Details Window

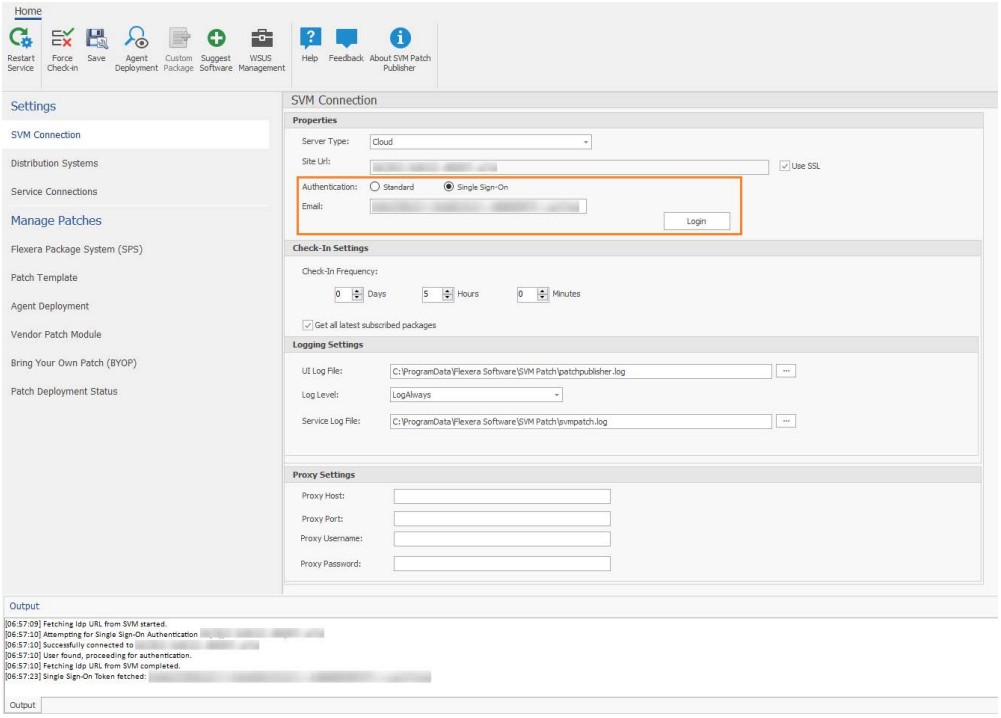
WSUS Management Tool Integration with SVM Patch Publisher

The WSUS Management tool is now integrated within the SVM Patch publisher. To launch the **WSUS Management Tool**, click on the **WSUS Management** button in the ribbon of the SVM Patch Publisher. As a prerequisite, the successful launching of the **WSUS Management Tool** will require the WSUS Administration Console to be installed on the device.



Support for SSO Authentication in SVM Connection

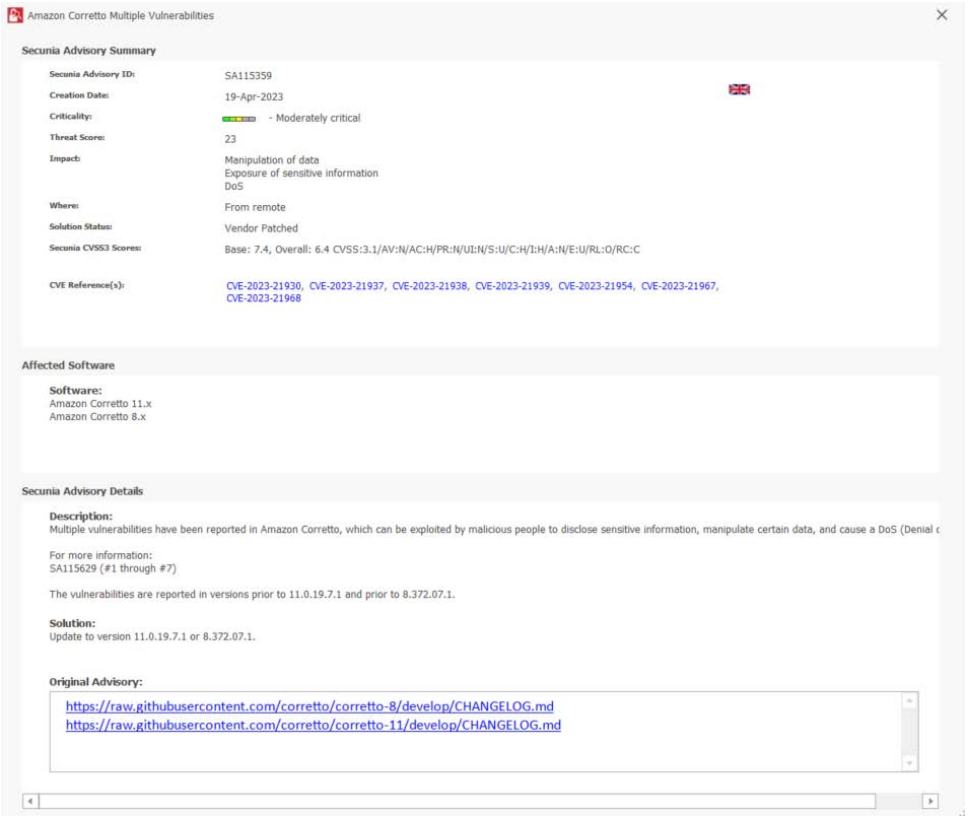
The SVM Patch Publisher now supports Single Sign-On for authentication. To do so, select the **Single Sign-On** option, provide your official email address, and click the **Login** button. Clicking on Login will automatically redirect you to the configured Identity Provider at your organization for login. Upon successful authentication, you will be connected to SVM in the Patch Publisher.



Hyperlinks in Advisory Details Window

In the Advisory details window, **CVE Reference** and **Secunia Advisory Details** links are now clickable.

- You can now click on any CVE listed in the **CVE Reference** section of the Advisory Details window to take you to its corresponding page on the cve.mitre.org website for more information.
- The URLs in the **Secunia Advisory Details** section can now be clicked to navigate to external websites for additional details.



Software Vulnerability Manager User Interface Enhancements

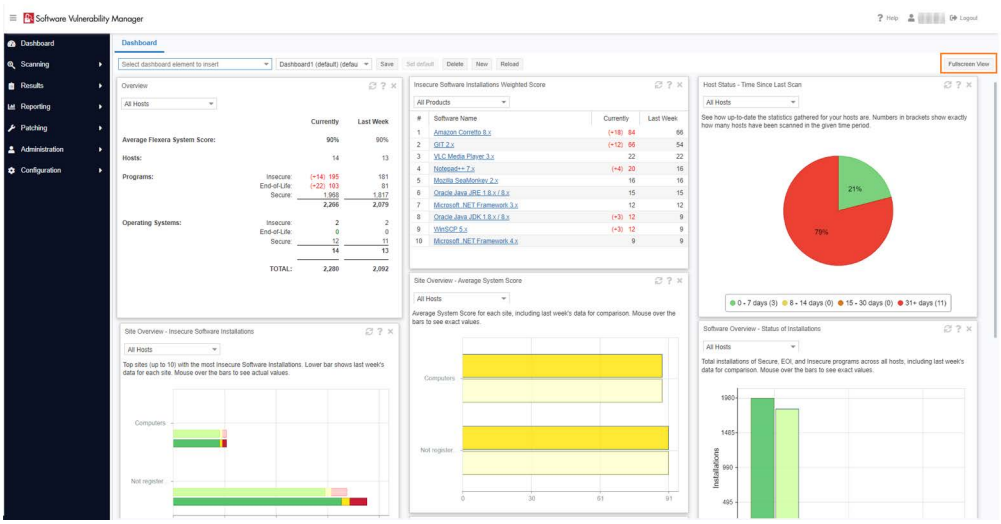
The following improvements have been added to the Software Vulnerability Manager User Interface.

- Dashboard Page Improvements
- Enhanced “Message” Column in Patch Deployment Status Grid

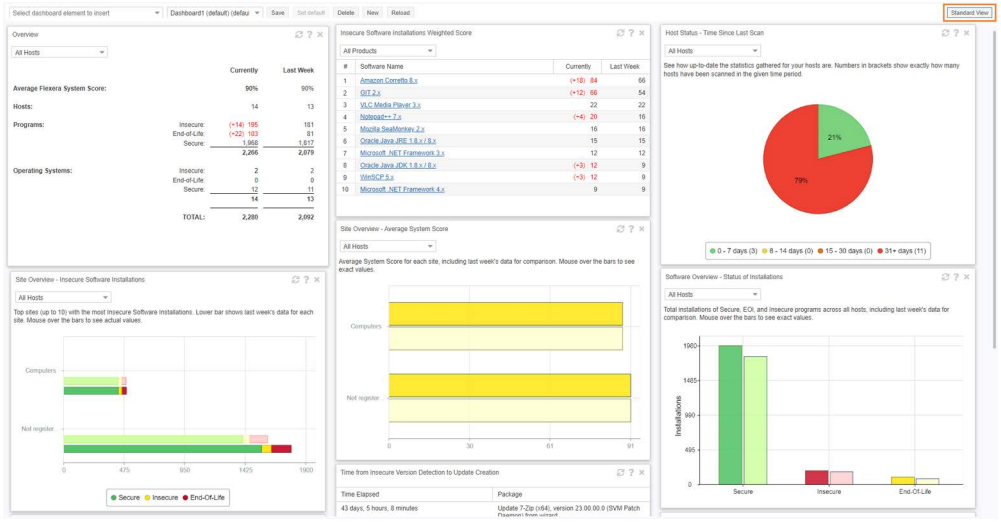
Dashboard Page Improvements

The following buttons have been added to the Dashboard page in the Software Vulnerability Manager console:

- **Fullscreen View—**Click the **Fullscreen View** button to view the Dashboard page on full screen.

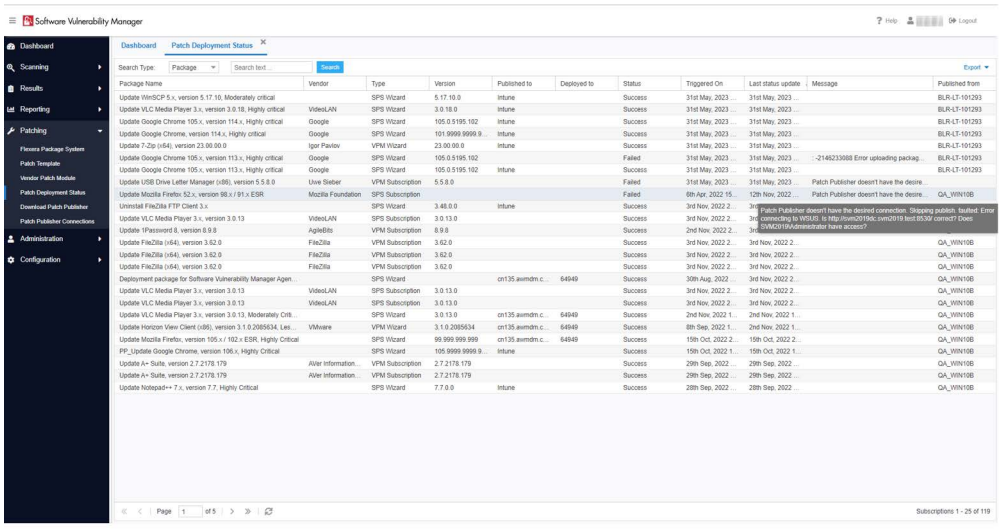


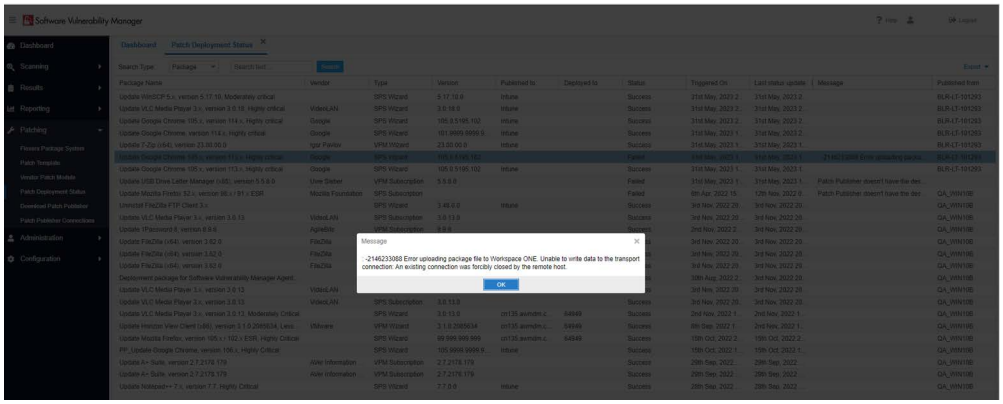
- **Standard View—**To exit the fullscreen view of the Dashboard page, click on the **Standard View** button.



Enhanced “Message” Column in Patch Deployment Status Grid

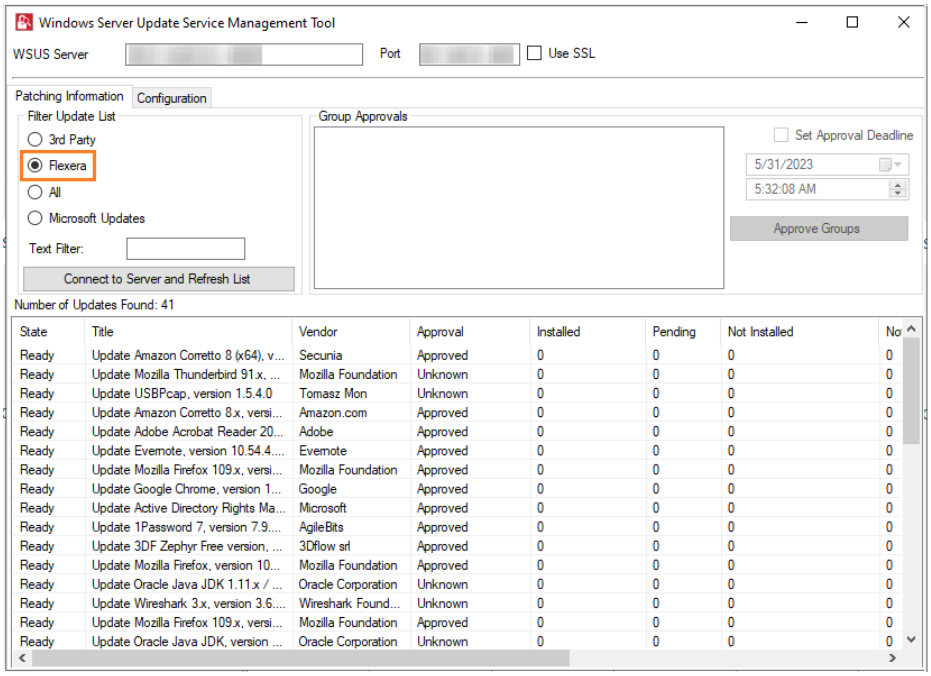
Upon mouse hovering on the **Message** column, you will see the entire message appear as a tooltip. Alternatively, you can click on the **Message** to see the entire message appear in a popup message box.





WSUS Management Tool Improvements

In the **WSUS Management Tool > Patching Information** tab, a new **Flexera** filter has been added to view the patches published to the WSUS from the SVM Patch Publisher/SVM console. To view the Flexera patches, select the **Flexera** filter option and click the **Connect to Server and Refresh List** button.



Reference: Latest Binary Versions

The following version of the binaries provided are:

- SVM ActiveX Plug-in v7.6.0.24 (no change)
- Single Host Agent v7.6.0.24 (no change)
- SVM Daemon v7.6.0.24 (no change)
- SVM System Center Plugin v7.6.0.24 (no change)
- SVM Patch Publisher v7.11.1009 (to download, click here)

  Refer “Patch Publisher Enhancements” for changelog.
- SVM Cloud Client Toolkit v5.0.561 (to download, click here) (no change)

  This toolkit contains offline utilities such as the Multi-partition Reporting Tool, WSUS Management Tool and Client Data Tool which add value to SVM. This toolkit does not consist of Patch Daemon. This toolkit is for SVM Cloud edition only.

Note • *The Flexera SVM Patch Configuration will be deprecated in the future; therefore, you are encouraged to migrate to the new SVM Patch Publisher tool.*

Known Issues

The following table lists the known issues in Software Vulnerability Manager (Cloud Edition):

Issue	Description
IOK-1041602	You may notice that the first user may not be completely logged out of SVM Patch Publisher, when the second user attempts to log into the same Patch Publisher. This behavior may be seen only when the 'Stay Signed In' or 'Remember Me' option is selected on the IDP login prompt that appears upon logging into Patch Publisher via SSO authentication.

Resolved Issues

The following table lists the customer issues that were resolved in Software Vulnerability Manager (Cloud Edition):

Issue	Description
SQ-1210	While deploying patches to Microsoft Intune, the failed message appears due to special characters in the path.
IOK-1040429	In SVM console, unable to save 'Flexera SPS Timestamp' in the Settings page.
IOK-1039958	VPM grid crashes on selecting the smart group filters.

Community Blogs

Please subscribe to latest posts about Software Vulnerability Manager by going to https://community.flexera.com/t5/Software-Vulnerability/bg-p/SoftwareVulnerabilityManagementblog and clicking on subscribe.

Please subscribe to latest release announcements concerning Software Vulnerability Manager by going to https://community.flexera.com/t5/Software-Vulnerability/bg-p/Software-Vulnerability-Release-blog and clicking on subscribe.

Product Feedback

Have a suggestion for how we can improve this product? Please share your feedback with the product team by visiting the Software Vulnerability Manager Forum in the Flexera Community:

https://community.flexera.com/t5/Software-Vulnerability/bd-p/SVM-Discussion

Legal Information

Copyright Notice

Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see https://www.flexera.com/legal/intellectual-property.html. All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.