

Software Vulnerability Manager (Cloud Edition) Release Notes

May 2023 - Update 2

Introduction	1
New Features and Enhancements	2
Patch Publisher Enhancements	2
WSUS Management Tool Integration with SVM Patch Publisher.....	2
Support for SSO Authentication in SVM Connection	3
Hyperlinks in Advisory Details Window	3
Software Vulnerability Manager User Interface Enhancements	4
Dashboard Page Improvements.....	4
Enhanced “Message” Column in Patch Deployment Status Grid	5
WSUS Management Tool Improvements	6
Reference: Latest Binary Versions.....	7
Known Issues	8
Resolved Issues.....	8
Community Blogs.....	8
Product Feedback	8
Legal Information	9

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.

The screenshot shows the SVM Patch Publisher interface. The ribbon at the top includes buttons for Home, Restart Service, Force Check-in, Save, Agent Deployment, Custom Package, Suggest Software, **WSUS Management** (highlighted with a red box), Help, Feedback, and About SVM Patch Publisher. The left sidebar contains settings for SVM Connection, Distribution Systems, Service Connections, Manage Patches, Flexera Package System (SPS), Patch Template, Agent Deployment, Vendor Patch Module, Bring Your Own Patch (BYOP), and Patch Deployment Status. The main area displays a table of patch data for the Flexera Package System (SPS).

Product	Patched Vers...	Vendor	Architecture	SAD	Criticality	Threat Score	Detected	Advisory Publ...	Insecure	End-Of-Life	Secure	Total	Hosts	Uninstallable
Intrepid+ 7.x	7.7		Windows 64...	SA91113	Highly critical	2	3 minutes ago	18th Septem...	4	0	0	4	4	No
Google Chrome	114.x	Google	Windows 64...	SA116725	Highly critical	15	3 minutes ago	31st May, 2023	1	7	0	8	7	No
Mozilla Firefox	113.x / 102.x...	Mozilla Foun...	Windows 64...	SA113921	Highly critical	23	3 minutes ago	09th May, 2023	0	10	0	10	7	Yes
WinRAR 3.x	3.6.x	WinRAR	Windows 64...				22 minutes a...		1	1	0	2	2	No
VLC Media PL...	3.0.18	VideoLAN	Windows 64...	SA112388	Highly critical	3	22 minutes a...	29th Novemb...	3	0	0	3	3	Yes
VLC Media PL...	3.0.18	VideoLAN	Windows 32...	SA112388	Highly critical	3	22 minutes a...	29th Novemb...	3	0	0	3	3	Yes
Mozilla Thun...	102.x	Mozilla Foun...	Windows 64...	SA116081	Highly critical	23	22 minutes a...	10th May, 2023	0	2	0	2	2	No
Apache Open...	4.1.14	OpenOffice.org	Windows 32...	SA114788	Highly critical	20	22 minutes a...	24th March...	2	0	0	2	2	No
LibreOffice 6.x	7.x	The Document...	Windows 32...				22 minutes a...		2	1	0	3	3	No
Oracle Java J...	11.0.19	Oracle Corp...	Windows 64...	SA115629	Highly critical	23	22 minutes a...	18th April, 20...	2	0	0	2	2	No
InfraView 4.x	4.60	InfraView	Windows 64...	SA107469	Highly critical	1	22 minutes a...	18th March...	1	0	0	1	1	Yes
InfraView 4.x	4.60	InfraView	Windows 32...	SA107469	Highly critical	1	22 minutes a...	18th March...	1	0	0	1	1	Yes
Mozilla Firefox	113.x / 102.x...	Mozilla Foun...	Windows 32...	SA113921	Highly critical	23	22 minutes a...	09th May, 2023	0	4	0	4	3	Yes
Amazon Cor...	8.372.07.1	Amazon.com	Windows 64...	SA113359	Highly critical	23	22 minutes a...	19th April, 20...	16	0	0	16	5	No
Adobe Acrobat...	23.x (Continu...	Adobe	Windows 32...	SA113343	Highly critical	12	22 minutes a...	11th April, 20...	1	5	0	6	6	No
Zoom Client F...	5.11.5	Zoom Video	Windows 32...	SA112726	Highly critical	18	8 days, 6 hou...	15th March...	1	0	0	1	1	No
Oracle Java J...	8u371	Oracle Corp...	Windows 64...	SA115629	Highly critical	23	8 days, 6 hou...	18th April, 20...	3	0	0	3	2	No
Google Chrome	114.x	Google	Windows 32...	SA116725	Highly critical	15	8 days, 6 hou...	31st May, 2023	1	1	0	2	2	No
Amazon Cor...	8.372.07.1	Amazon.com	Windows 32...	SA113359	Highly critical	23	8 days, 6 hou...	19th April, 20...	12	0	0	12	4	No

Output

```
[17:20:41] Fetching smart groups list from SVM completed.
[17:20:41] Fetching Patch template list from SVM started.
[17:20:42] Fetching patch template list from SVM completed.
```

Support for SSO Authentication in SVM Connection

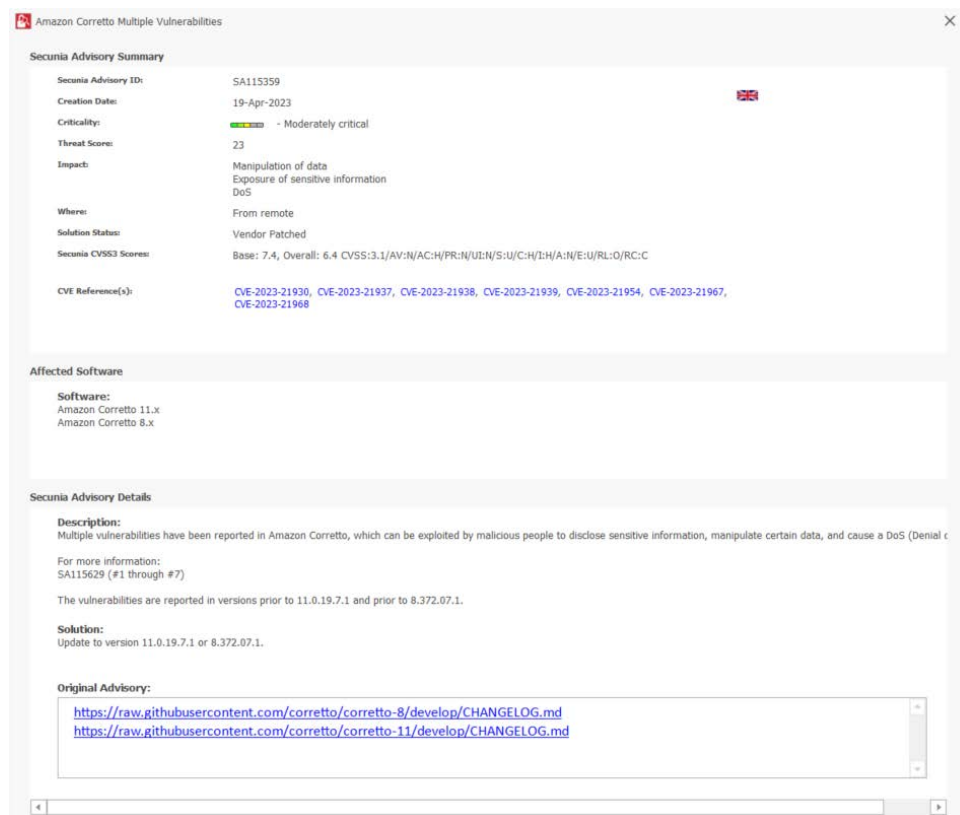
The SVM Patch Publisher now supports Single Sign-On for authentication. To do so, select the **Single Sign-On** option, provide your official email address, and click the **Login** button. Clicking on Login will automatically redirect you to the configured Identity Provider at your organization for login.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

The screenshot shows the 'SVM Connection' settings window. The 'Authentication' section is highlighted with an orange box, showing the 'Single Sign-On' radio button selected. Below it, there is an 'Email' input field and a 'Login' button. The 'Check-In Settings' section shows a frequency of 0 days, 5 hours, and 0 minutes, with a checkbox for 'Get all latest subscribed packages' checked. The 'Logging Settings' section shows the 'Log Level' set to 'LogAlways'. The 'Proxy Settings' section has empty input fields for 'Proxy Host', 'Proxy Port', 'Proxy Username', and 'Proxy Password'. The 'Output' section at the bottom shows a log of events, including 'Fetching idp URL from SVM started', 'Attempting for Single Sign-On Authentication', 'Successfully connected to', 'User found, proceeding for authentication', 'Fetching idp URL from SVM completed', and 'Single Sign-On Token fetched'.

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

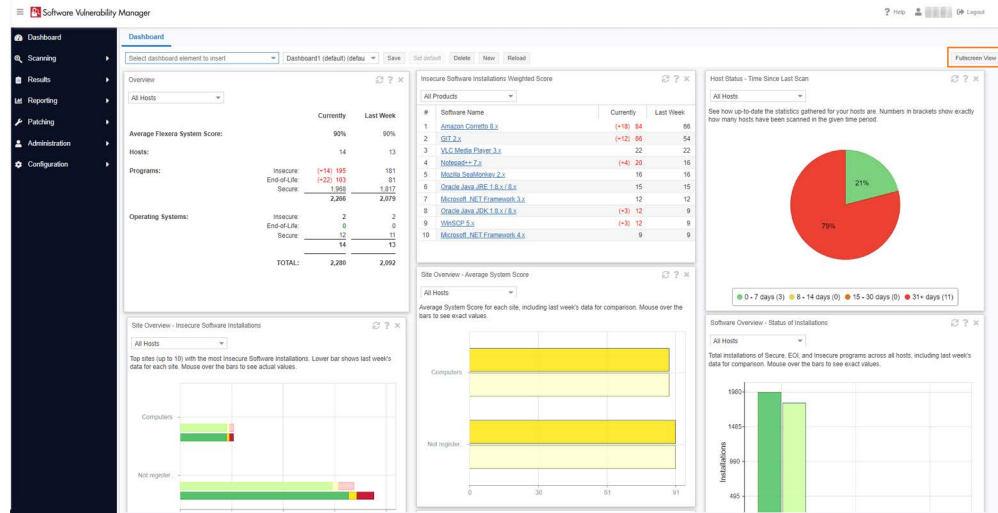
The following improvements have been added to the Software Vulnerability Manager User Interface.

- [Dashboard Page Improvements](#)
- [Enhanced “Message” Column in Patch Deployment Status Grid](#)

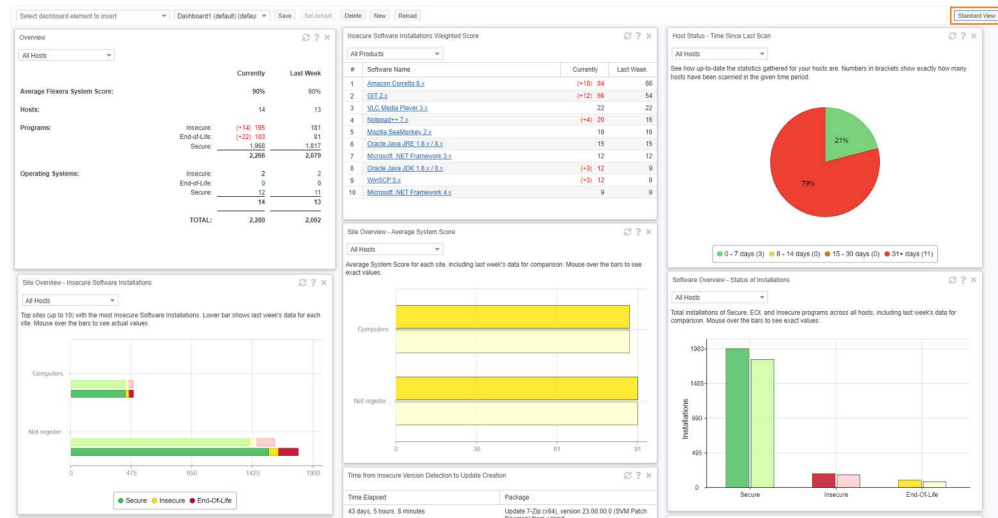
Dashboard Page Improvements

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.



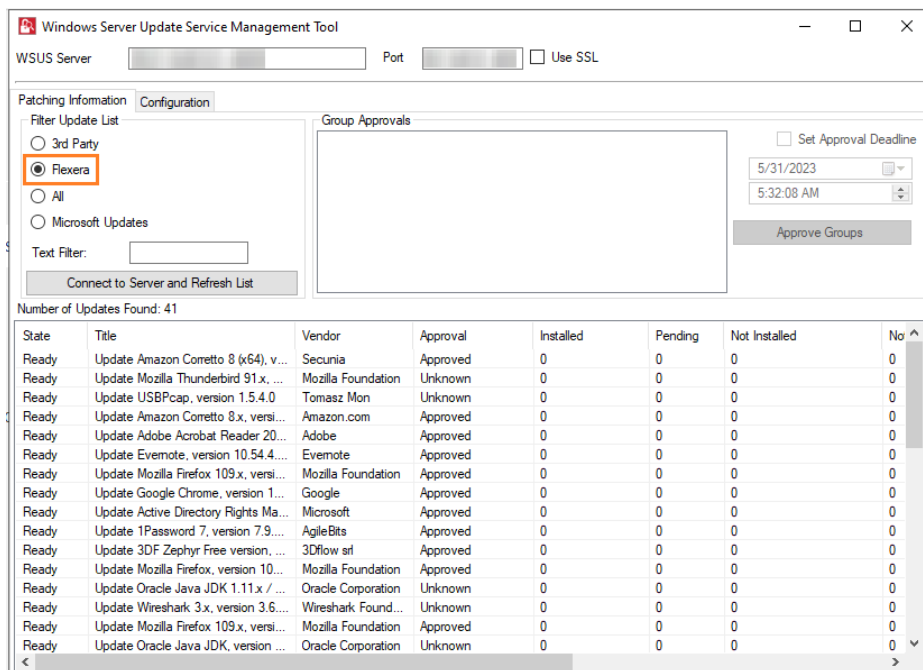
Enhanced “Message” Column in Patch Deployment Status Grid

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.

[illegible][illegible]

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

Copyright © 2023 Flexera

This publication contains proprietary and confidential information and creative works owned by Flexera and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera is strictly prohibited. Except where expressly provided by Flexera in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera intellectual property rights, whether by estoppel, implication, or otherwise.

All copies of the technology and related information, if allowed by Flexera, must display this notice of copyright and ownership in full.

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.