Software Vulnerability Manager (On-Premises Edition) Release Notes

July 2023

Introduction .................................................................................................................................... 1

New Features and Enhancements ...................................................................................................... 2
  Patch Publisher Enhancements ........................................................................................................... 2
    Support for SSO Authentication in SVM Connection ................................................................. 2
    WSUS Management Tool Integration with SVM Patch Publisher ............................................... 3
  Vendor Patch Module View Enhancements .................................................................................... 3
  Group Products Based on Patched Version in the Flexera Package System (SPS) View .......... 5
  Export Option in Patch Publisher Grids ........................................................................................ 5
  Search Option in Applicability Criteria - Paths Panel ................................................................. 6
  Average Resolution Time in the SVM Software Suggestion Tool ................................................ 6
  Software Vulnerability Manager User Interface Enhancements .................................................. 7
    Dashboard Page Improvements .................................................................................................. 7
    Average Resolution Time on the Software Suggestion Page ..................................................... 8
    Installations Tab Improvements in Smart Groups .................................................................. 9
    Smart Groups Compilation Improvements ............................................................................. 10
    “Last Logged In” Column in User Management Grid ................................................................. 10
    Enhanced “Message” Column in Patch Deployment Status Grid ........................................... 11
  WSUS Management Tool Improvements ..................................................................................... 12
    Hyperlinks in Advisory Details Window ................................................................................... 12
    Reference: Latest Binary Versions ............................................................................................ 14

Known Issues................................................................................................................................. 14

Resolved Issues ............................................................................................................................ 15

Community Blogs.......................................................................................................................... 15

Product Feedback ......................................................................................................................... 15

Legal Information .......................................................................................................................... 15
Introduction

Flexera’s Software Vulnerability Manager (formerly called Software Vulnerability Manager 2019) is a vulnerability and patch management software solution that facilitates a customized patch management process. It combines vulnerability intelligence, vulnerability scanning, and patch creation with patch deployment tool integration to enable targeted, reliable, and cost-efficient patch management.

Vulnerability and patch management are critical components of any security infrastructure because they enable proactive detection and remediation of vulnerabilities before they are actively exploited and your security compromised. With Software Vulnerability Manager, IT operations and security teams are empowered to prevent vulnerability threats from both Microsoft and non-Microsoft (third-party) product vulnerabilities, covering Microsoft Windows, macOS, and Red Hat Enterprise Linux.

Software Vulnerability Manager integrates seamlessly with Microsoft® WSUS and System Center Configuration Manager via Microsoft® Intune, VMware® Workspace One, or BigFix.

New Features and Enhancements

Software Vulnerability Manager (On-Premises Edition) includes the following new features and enhancements:

- Patch Publisher Enhancements
- Software Vulnerability Manager User Interface Enhancements
- WSUS Management Tool Improvements
- Hyperlinks in Advisory Details Window
- Reference: Latest Binary Versions

Note • To see the following new features and enhancements in your Software Vulnerability Manager (On-Premises 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.

- Support for SSO Authentication in SVM Connection
- WSUS Management Tool Integration with SVM Patch Publisher
- Vendor Patch Module View Enhancements
- Group Products Based on Patched Version in the Flexera Package System (SPS) View
- Export Option in Patch Publisher Grids
- Search Option in Applicability Criteria - Paths Panel
- Average Resolution Time in the SVM Software Suggestion Tool
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.

![Support for SSO Authentication in SVM Connection](image)

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.
Vendor Patch Module View Enhancements

Following enhancements are added to the Vendor Patch Module > Configuration View:

- **Select Package Language**—In the Configuration View dialog, the Select Package Language property has been added. With this update you can now change the default selected language and select new package language. To do so, click ellipses (…) button, select the desired language in the Select Package Language dialog box, and then click OK button.

- **Highlight the Published Products**—In the Configuration View dialog, the Highlight product for which update packages have been created option is now enabled to check/unchecked to highlight the products for which update packages have been created.
Group Products Based on Patched Version in the Flexera Package System (SPS) View

In the Flexera Package System (SPS) > Configuration View dialog, the **Group products where patched version and architecture are identical** option is now enables you to group the products based on Patched Version and Architecture.
Export Option in Patch Publisher Grids

A new **Export** button is introduced in the Flexera Package System (SPS), Patch Template, Vendor Patch Module (VPM), Bring Your Own Patch (BYOP), and Patch Deployment Status overview page.

You can choose to export data in the grid to a CSV file using the export feature that is built into each view.

Search Option in Applicability Criteria - Paths Panel

A new **Find** box is introduced in the Applicability Criteria - Paths panel of the Create Update Package Wizard. You can enter keywords in the **Find** box to find the matching applicability paths.
Average Resolution Time in the SVM Software Suggestion Tool

In the SVM Software Suggestion Tool window, you now have the ability to view the average resolution time for addressing the suggested software.
Software Vulnerability Manager User Interface Enhancements

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

- Dashboard Page Improvements
- Average Resolution Time on the Software Suggestion Page
- Installations Tab Improvements in Smart Groups
- Smart Groups Compilation Improvements
- “Last Logged In” Column in User Management Grid
- 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.
Average Resolution Time on the Software Suggestion Page

On the Software Suggestion page, you now have the ability to view the average resolution time for addressing the suggested software.

Installations Tab Improvements in Smart Groups

Following enhancements are added in Smart Groups > View Installations context menu > Installations tab:

- **Search**—Under Installations tab, a new **Search** box has been added. You can now enter keywords in the **Search** box to search for the matching hosts in the grid.
• **Copy path to clipboard**— Under Installations tab, you can now copy the selected installation path of a file to the clipboard. To do so, right click on selected row and choose **Copy path to clipboard**.

---

**Smart Groups Compilation Improvements**

Check boxes have been added in Create & Edit grid of Host Smart Groups/Product Smart Groups/Advisory Smart Groups to support complication of multiple smart groups at once. By clicking check boxes by multiple smart groups, you can initiate compilation of one or more smart groups at a time.
“Last Logged In” Column in User Management Grid

A new Last Logged In column has been added to the User Management grid. The Last Logged In column now displays last successful login to the application.

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.
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.
### Amazon Corretto Multiple Vulnerabilities

#### Secunia Advisory ID:
SA113414

#### Creation Date:
2023-01-18

#### Criticality:
- Moderately critical

#### Threat Score:
7

#### Impact:
Manipulation of data

#### Where:
From remote

#### Solution Status:
Vendor Patched

#### Affected Software
Amazon Corretto 11.x
Amazon Corretto 8.x

#### Secunia Advisory Details
Multiple vulnerabilities have been reported in Amazon Corretto, which can be exploited by malicious people to manipulate certain data and cause a DoS (Denial of Service).

For more information:
SA113442 (#1 through #3)

The vulnerabilities are reported in versions prior to 11.0.18.10.1 and prior to 8.362.08.1.

#### Solution
Update to version 11.0.18.10.1 or version 8.362.08.1.

#### Original Advisory
- [https://github.com/amazon-aspentech/CHANGELOG.md](https://github.com/amazon-aspentech/CHANGELOG.md)
- [https://github.com/amazon-aspentech/CHANGELOG.md](https://github.com/amazon-aspentech/CHANGELOG.md)

#### Other References
SA113442
Reference: Latest Binary Versions

The following version of the binaries provided are:

- SVM ActiveX Plug-in v7.6.1.24 (no change)
- Single Host Agent v7.6.1.24 (no change)
- SVM Daemon v7.6.1.24 (no change)
- SVM System Center Plugin v7.6.1.24 (no change)
- SVM Patch Publisher v7.12.1042 (to download, click here)
  Refer “Patch Publisher Enhancements” for changelog.
- SVM On-Prem Client Toolkit v5.0.547 (to download, click here) (no change)

Known Issues

The following table lists the known issues in Software Vulnerability Manager (On-Premises Edition):

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOK-1038181</td>
<td>SSO redirects to old UI.</td>
</tr>
</tbody>
</table>
Resolved Issues

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

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOK-1021394</td>
<td>In Host Smart Groups &gt; Create and Edit grid, the View Smart Group Contents option is not working.</td>
</tr>
<tr>
<td>IOK-757345</td>
<td>Display proper messages on submitting Software Suggestion.</td>
</tr>
<tr>
<td>IOK-1012233</td>
<td>While deploying patches to Microsoft Intune, the failed message appears due to special characters in the path.</td>
</tr>
<tr>
<td>IOK-1040429</td>
<td>In SVM console, unable to save 'Flexera SPS Timestamp' in the Settings page.</td>
</tr>
<tr>
<td>IOK-1039958</td>
<td>VPM grid crashes on selecting the smart group filters.</td>
</tr>
</tbody>
</table>

Community Blogs

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