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, endpoint 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
- 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.

- Export Option in Patch Publisher Grids
- Search Option in Applicability Criteria - Paths Panel
- Highlight the Published Products in the Vendor Patch Module View
- Average Resolution Time in the SVM Software Suggestion Tool
- Group Products Based on Patched Version in the Flexera Package System (SPS) View

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.

Highlight the Published Products in the Vendor Patch Module View

In the Vendor Patch Module > Configuration View dialog, the **Highlight product for which update packages have been created** option is now enabled to check/uncheck to highlight the products for which update packages have been created.
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.

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.
Software Vulnerability Manager User Interface Enhancements

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

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

**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.
“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.

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**.

---

**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 v7.12.1039 (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):

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOK-1047113</td>
<td>Ungrouped patch creation have missing values in the wizard.</td>
</tr>
</tbody>
</table>

Resolved Issues

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

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOK-757345</td>
<td>Display proper messages on submitting Software Suggestion.</td>
</tr>
</tbody>
</table>

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.


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.