Software Vulnerability Manager (Cloud Edition) Release Notes

August 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.

SVM Patch Publisher inherits its current functionalities from the Patch Daemon. SVM Patch Publisher enables you to configure connections to the SVM server and to the supported end point management systems. The tool polls SVM on a configured frequency to look for new patches resulting either from a manual publish or Patch Automation to publish patches to the specified end point management system.

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).*

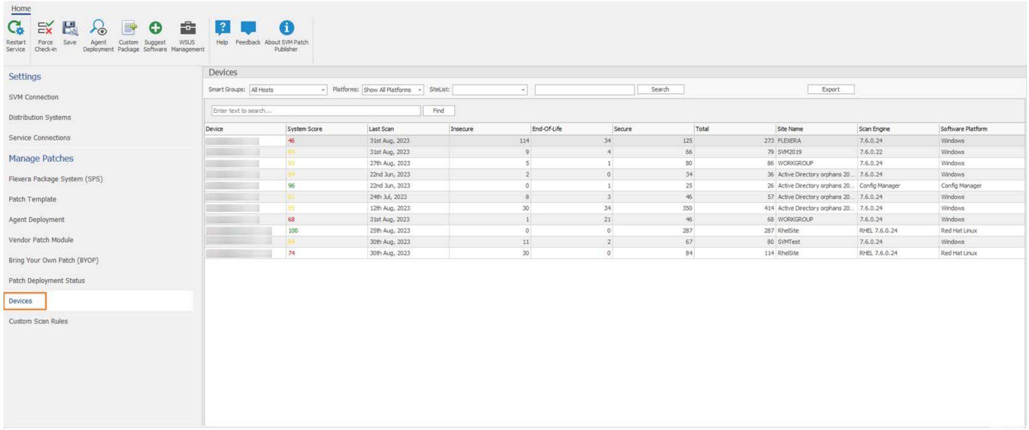
Patch Publisher Enhancements

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

- Devices View
- Highlight the Published Products in the Flexera Package System (SPS) View

Devices View

A new **Devices** view is introduced under the **Manage Patches** menu. The **Devices** view displays the hosts/devices based on the Host Smart Group that is selected from the **Smart Group** drop-down.



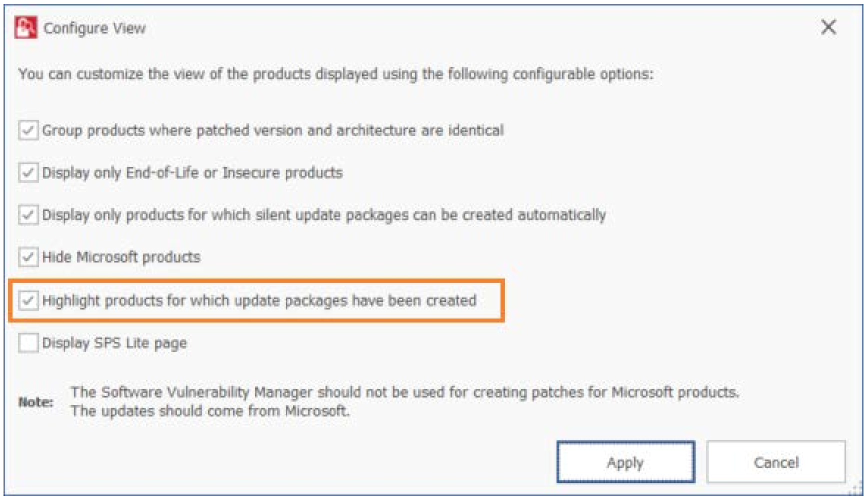
Devices

Smart Groups: All Hosts   Platforms: Show All Platforms   SiteList:

Device	System Score	Last Scan	Insecure	End-Of-Life	Secure	Total	Site Name	Scan Engine	Software Platform
[redacted]	46	31st Aug, 2023	114	34	125	273	FLEXERA	7.6.0.24	Windows
[redacted]	89	31st Aug, 2023	9	4	66	79	SVM2019	7.6.0.22	Windows
[redacted]	93	27th Aug, 2023	5	1	80	86	WORKGROUP	7.6.0.24	Windows
[redacted]	94	22nd Jun, 2023	2	0	34	36	Active Directory orphans 20...	7.6.0.24	Windows
[redacted]	96	22nd Jun, 2023	0	1	25	26	Active Directory orphans 20...	Config Manager	Config Manager
[redacted]	81	24th Jul, 2023	8	3	46	57	Active Directory orphans 20...	7.6.0.24	Windows
[redacted]	85	12th Aug, 2023	30	34	350	414	Active Directory orphans 20...	7.6.0.24	Windows
[redacted]	68	31st Aug, 2023	1	21	46	68	WORKGROUP	7.6.0.24	Windows
[redacted]	100	25th Aug, 2023	0	0	287	287	RhelSite	RHEL 7.6.0.24	Red Hat Linux
[redacted]	84	30th Aug, 2023	11	2	67	80	SVMTest	7.6.0.24	Windows
[redacted]	74	30th Aug, 2023	30	0	84	114	RhelSite	RHEL 7.6.0.24	Red Hat Linux

Highlight the Published Products in the Flexera Package System (SPS) View

In the **Flexera Package System (SPS) > Configuration View** dialog box, the **Highlight product for which update packages have been created** option is now enabled to check/uncheck to highlight the products for which an update package is created and published to a configured endpoint management system.



Configure View

You can customize the view of the products displayed using the following configurable options:

☑ Group products where patched version and architecture are identical

☑ Display only End-of-Life or Insecure products

☑ Display only products for which silent update packages can be created automatically

☑ Hide Microsoft products

☑ Highlight products for which update packages have been created

□ Display SPS Lite page

Note: The Software Vulnerability Manager should not be used for creating patches for Microsoft products. The updates should come from Microsoft.

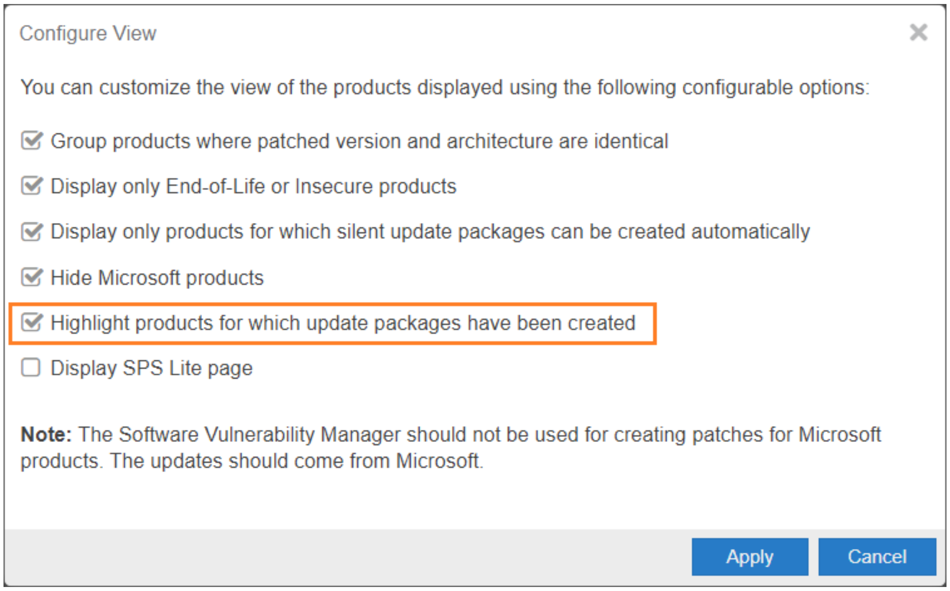
Software Vulnerability Manager User Interface Enhancements

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

- Highlight the Published Products in the Flexera Package System (SPS) View

Highlight the Published Products in the Flexera Package System (SPS) View

In the **Flexera Package System (SPS) > Configuration View** dialog box, the **Highlight product for which update packages have been created** option is now enabled to check/uncheck to highlight the products for which update package is created and published to a configured endpoint management system.



Configure View

You can customize the view of the products displayed using the following configurable options:

☑ Group products where patched version and architecture are identical

☑ Display only End-of-Life or Insecure products

☑ Display only products for which silent update packages can be created automatically

☑ Hide Microsoft products

☑ Highlight products for which update packages have been created

□ Display SPS Lite page

Note: The Software Vulnerability Manager should not be used for creating patches for Microsoft products. The updates should come from Microsoft.

Reference: Latest Binary Versions

The following is the list of binaries versions:

- 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 v7.14.1063 (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-1058093	When certain special characters are used in password, Client Data tool gives “Invalid Credentials”.

Resolved Issues

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

Issue	Description
IOK-1055008	On Creating/Editing the Patch Template, updated message in the output window saying template created/updated successfully.
IOK-105162	Fixed Type 3 scans on machines with large installation paths.

Community Blogs

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

Please subscribe to the 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 **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

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.