Software Vulnerability Manager (Cloud Edition) Release Notes

September 2022

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 or VMware® Workspace One.

New Features and Enhancements

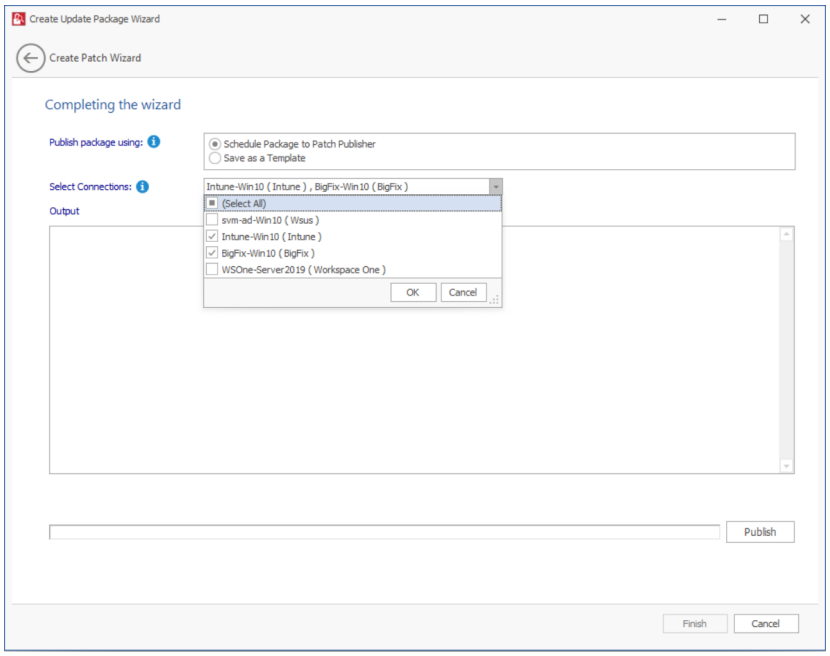
Software Vulnerability Manager (Cloud Edition) includes the following new features and enhancements:

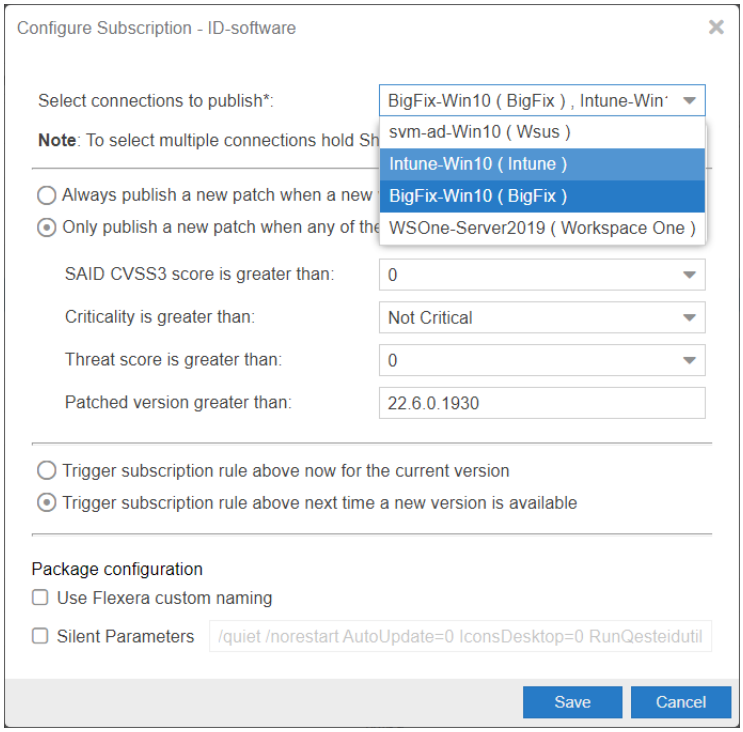
- Publish Patches to Multiple Endpoint Management Systems Simultaneously
- Scan Cloud Storage Solutions like OneDrive, Dropbox etc., Without Triggering Downloads
- Binary Versions

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).*

Publish Patches to Multiple Endpoint Management Systems Simultaneously

With this release, you can now publish patches (SPS and VPM) to more than one endpoint management system (or tenant) at the same time. Selecting of multiple connections will also be possible for QuickPatch and while subscribing patches for automation.





Scan Cloud Storage Solutions like OneDrive, Dropbox etc., Without Triggering Downloads

Windows and Mac scan agents will not download the online-only files during scanning. Such files will not be seen in the scan result as those files will not be physically available on the end point.

Binary Versions

The following version of the binaries provided are:

- SVM ActiveX Plug-in v7.6.0.22
- Single Host Agent v7.6.0.22
- SVM Daemon v7.6.0.22 (no feature update)
- SVM System Center Plugin v7.6.0.22 (no feature update)
- SVM Patch Publisher v7.4.797 (to download, click here)
- 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.

  Patch Daemon 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-704176	When connection to Intune is established for the first time with an App Category, publishing of SPS and VPM patches to this Intune connection will fail. Please follow the below steps for the workaround: ● Delete the configured App Category and save the Intune connection. ● Publish at least one patch to the Intune connection without App Category. ● Reconfigure the Intune connection with the App Category. Now all patch publishes to Intune should work.
IOK-884662	SPS and Products Smartgroups grids performance degradation.

Resolved Issues

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

Issue	Description
IOK-930101	Red Hat RPMs Wrongfully Listed as EOL.
IOK-882886	Patch Publisher - BigFix looping issue while publishing.
IOK-930778	VPM package special version consideration for publishing.

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 © 2022 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.