Software Vulnerability Manager (Cloud Edition) Release Notes

February 2023

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:

- Patch Publisher Enhancements

- Support for RHEL 9 Scanning

- 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.

- Support for Publishing Mac Packages to Microsoft Intune

- Support for Multiple Email Address in Software Suggestions
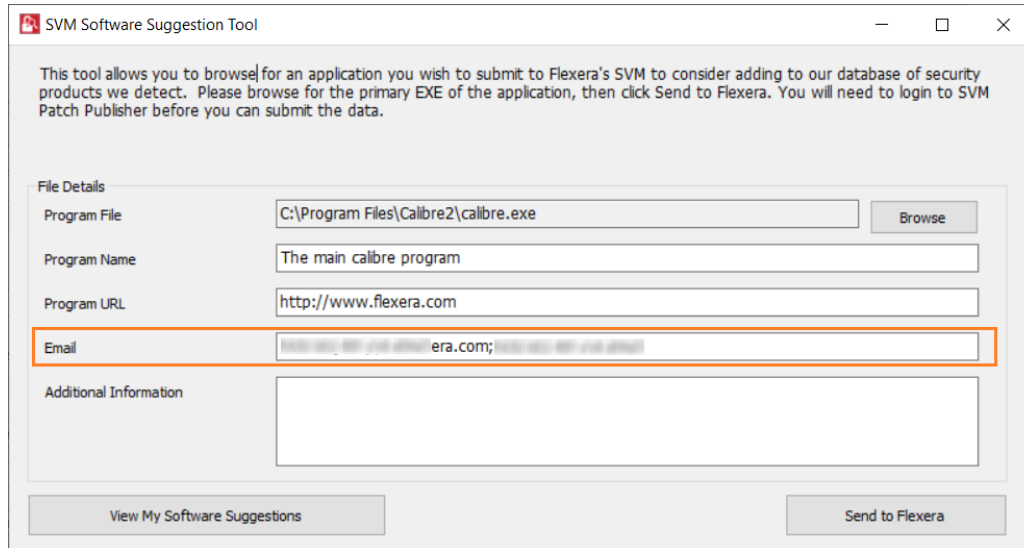
- Flexera Package System (SPS) View Enhancements

Support for Publishing Mac Packages to Microsoft Intune

In the Vendor Patch Module view of the SVM Patch Publisher, you can now publish the Mac packages (.PKG type) to the Microsoft Intune. To do so, right click on any Mac package (.PKG type), and then select **Create Update Package** from the context menu. Also, the Mac packages (.PKG type) that have the **Deployment Ready** status set to **Yes**, can be subscribed for automation.

## Support for Multiple Email Address in Software Suggestions

With this release, you can now add multiple email addresses while suggesting a software. The specified email addresses must be separated by either a comma (,) or a semi-colon (;).

Flexera Package System (SPS) View Enhancements

Following enhancements are added to Flexera Package System (SPS) view:

- **Search Type Field—** In the Flexera Package System (SPS) view, you can now search for SPS patches either by **Product** or **CVE**. You can also enter keywords in the **Find** box to find the matching entries in the grid.
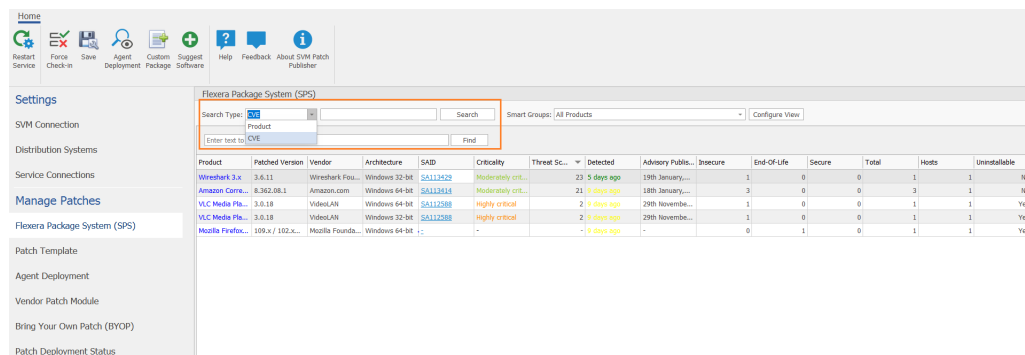
- **Enhanced Criticality Column—** The **Criticality** column now displays the color code depending upon the severity of a Secunia Advisory (SAID).
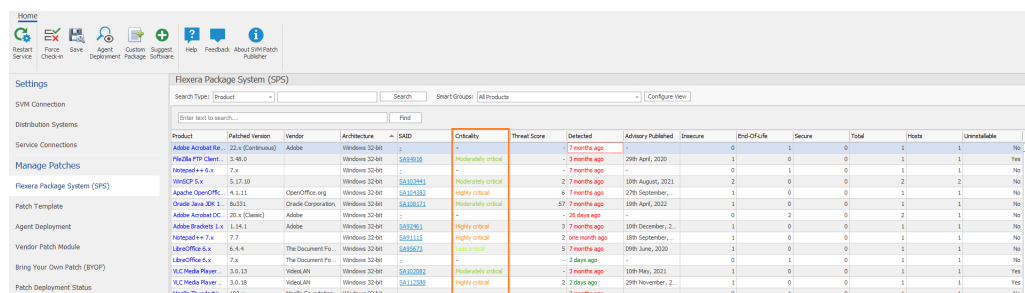
- **Secunia Advisory Details Popup—** By clicking on any **Secunia Advisory (SAID)**, a popup appears with the CVE, CVSS scores, affected software's, and other advisory details.

- **Enhanced Detected Column—** The **Detected** column now displays the number of minutes/hours/days/months of how long ago the vulnerabilities were detected in a scan.

Support for RHEL 9 Scanning

The SVM Single Host Agent v7.6.0.24 (scan agent) now supports scanning of Red Hat Enterprise Linux (RHEL) 9 Operating System.

Binary Versions

The following version of the binaries provided are:

- SVM ActiveX Plug-in v7.6.0.24

- Single Host Agent v7.6.0.24

- SVM Daemon v7.6.0.24

- SVM System Center Plugin v7.6.0.24

- SVM Patch Publisher v7.7.870 (to download, click here)

  Refer "New Features and 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.*

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.