Software Vulnerability Manager (On-Premises Edition) Release Notes

April 2023

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
- Removed RSAT as a Dependency for Installing SVM Patch Publisher
- Support for RHEL 9 Scanning
- Search Published Patch by Bulletin ID
- 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).
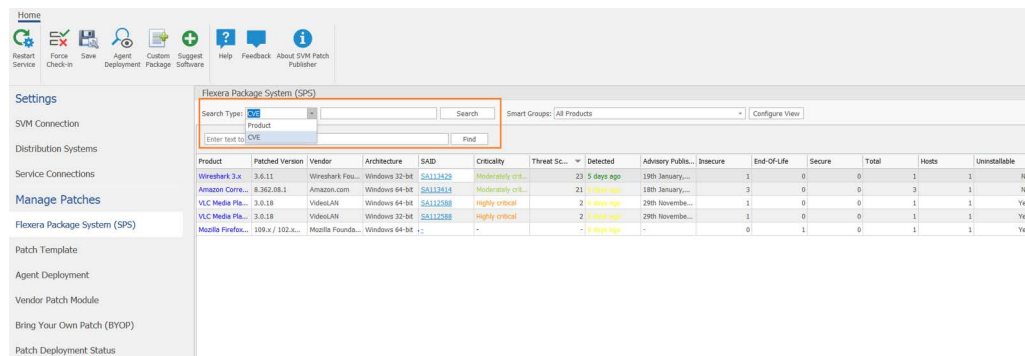
Patch Publisher Enhancements

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

- Support for Publishing Mac Packages to Microsoft Intune
- Support for Multiple Email Address in Software Suggestions
- Flexera Package System (SPS) View Enhancements
- Vendor Patch Module (VPM) View Enhancements
- "Download" Column in Bring Your Own Patch (BYOP) View
- Package Contents Panel Enhancements
- Add Multiple File Paths using a CSV File

### 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.
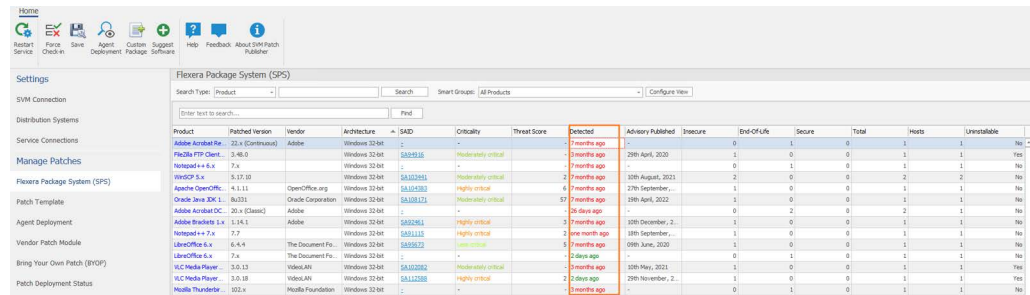
Support for Multiple Email Address in Software Suggestions

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).
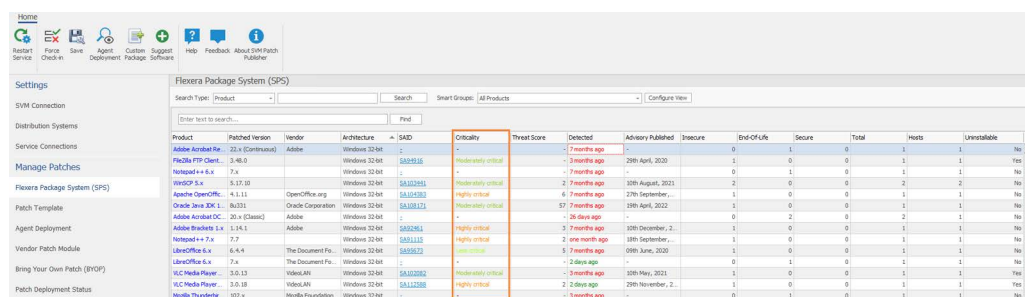
- **Secunia Advisory Details Popup—** By clicking on any **Secunia Advisory (SAID)**, a popup appears with the CVE, CVSS scores, affected software's, and other advisory details.
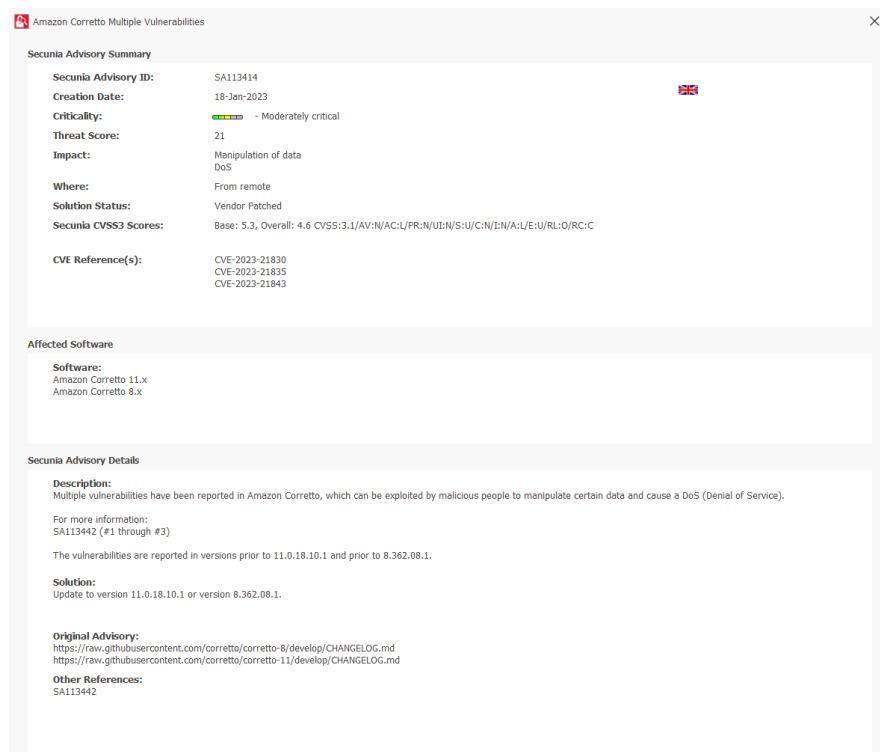
- **Enhanced Detected Column—** The **Detected** column now displays the number of minutes/hours/days/months of how long ago the vulnerabilities were detected in a scan.

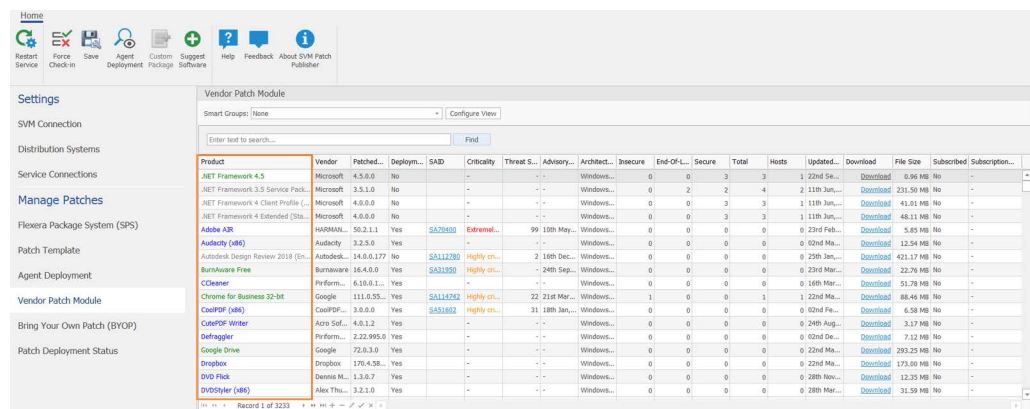

Vendor Patch Module (VPM) View Enhancements

Following enhancements are added to Vendor Patch Module (VPM) view:

- **Download Column—** The new **Download** column has been added in the VPM grid. Clicking on the **Download** link will downloaded the patch.
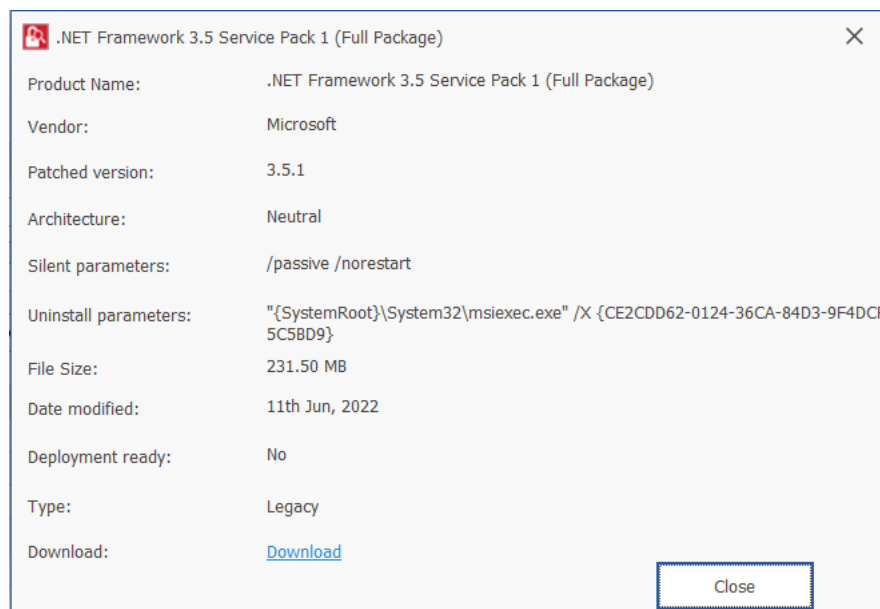

- **Highlighting Deployed Patches—** The patches that are published to a configured endpoint management system will be displayed in green color.

- **Enhanced Patch Information—** The Patch Information dialog box now displays the entire Silent and Uninstall parameters.

"Download" Column in Bring Your Own Patch (BYOP) View

A new **Download** column has been added to the BYOP grid. Clicking on the **Download** link will download the patch.
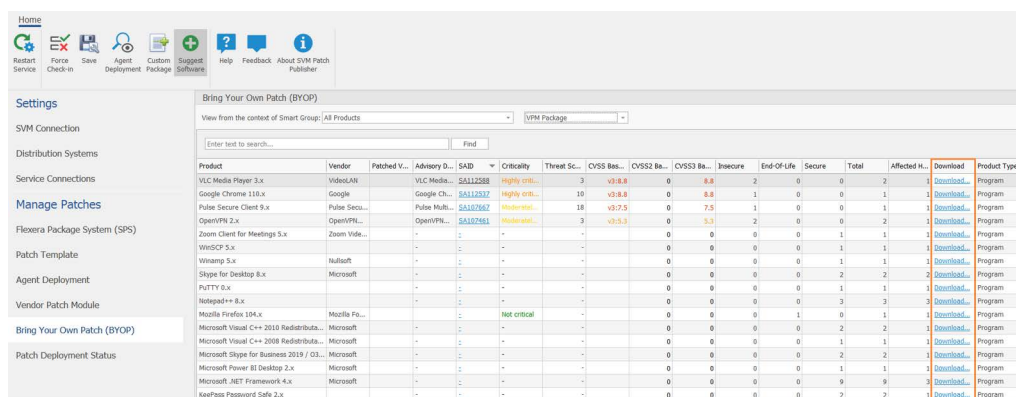
Package Contents Panel Enhancements

Following enhancements are added to **Package Contents** panel of the **Create Update Package Wizard**:

- **Language Aware Installation Option—**The **Language Aware Installation** option is now enabled for selection. This option is applicable only for the patches that support multiple languages. When **Language Aware Installation** is checked for a patch, the same language patch will be installed on an endpoint as that of the currently installed version of the product on that endpoint.
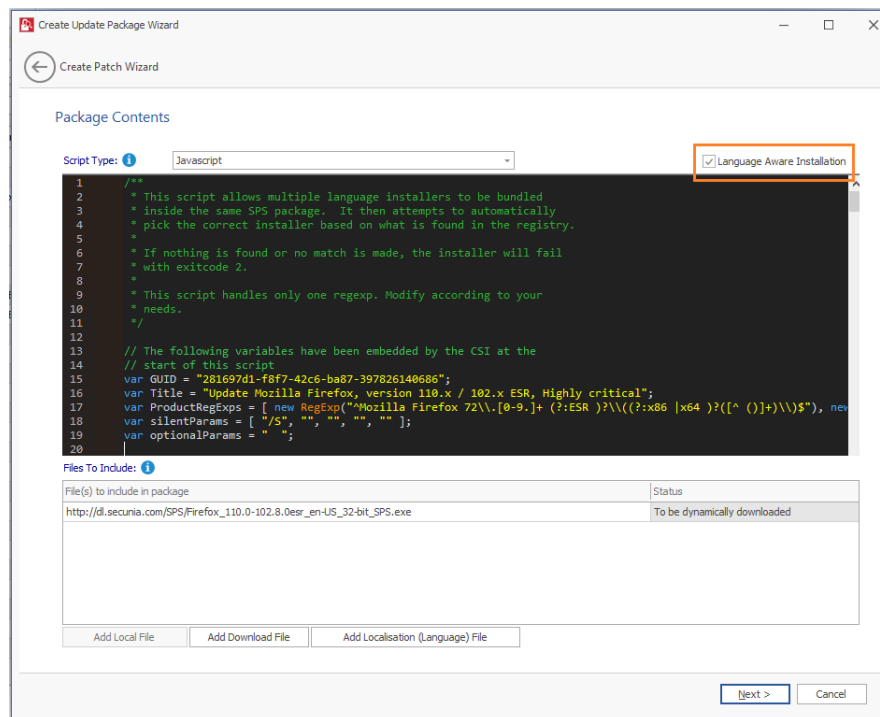
- **PowerShell and VBScript—**You can now see and edit the installation script of a patch as the newly added PowerShell Script or VBScript along with the existing JavaScript in the Script Type.
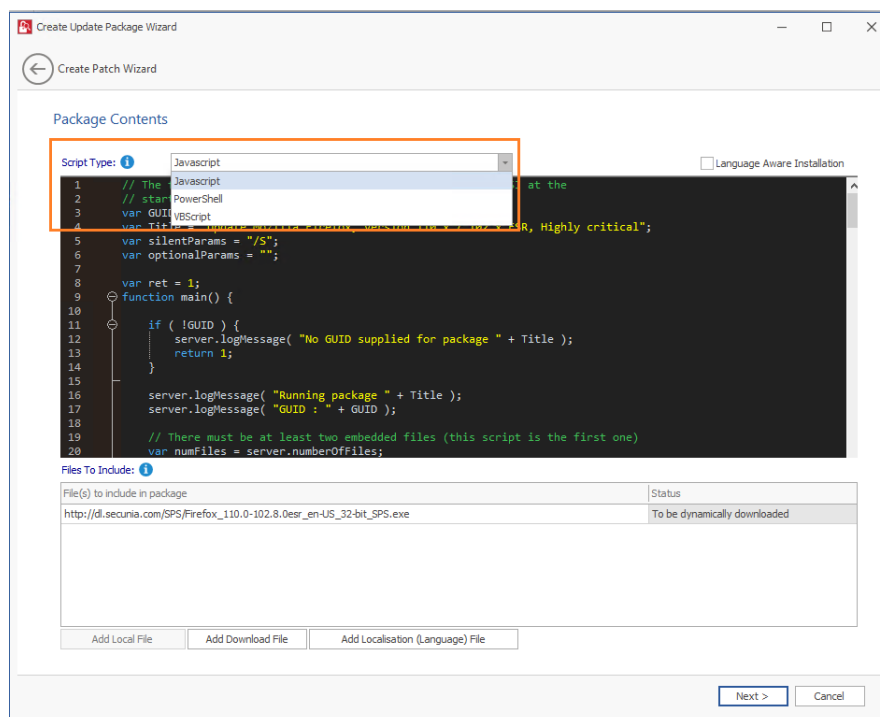
- **Download SPS File Option—**A new **Download SPS File** button is introduced to download the SPS file for the patch that is being published. By clicking on the button, the SPS file for the patch will be downloaded. Upon downloading the SPS file, the file path link will be displayed in the **SPS File Location** field.
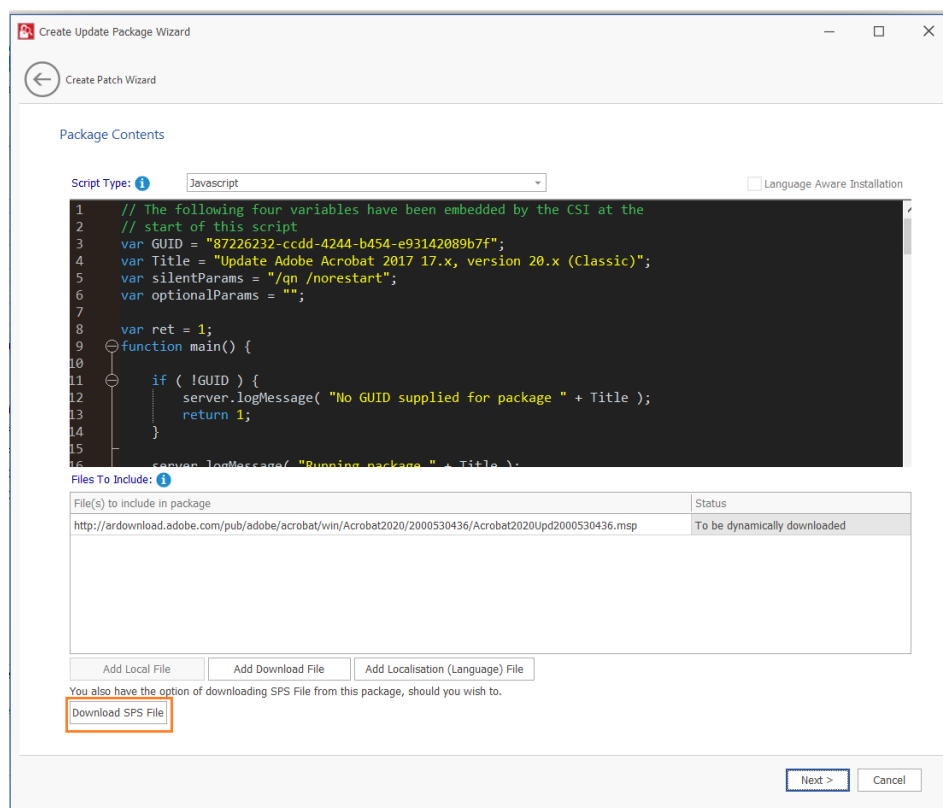
Add Multiple File Paths using a CSV File

A new **Import Paths** button is introduced in the **Applicability Criteria - Paths** panel of the **Create Update Package Wizard**, to add multiple file paths at once using a CSV file. The file paths imported in this panel will serve as applicability criteria for a patch during deployment.
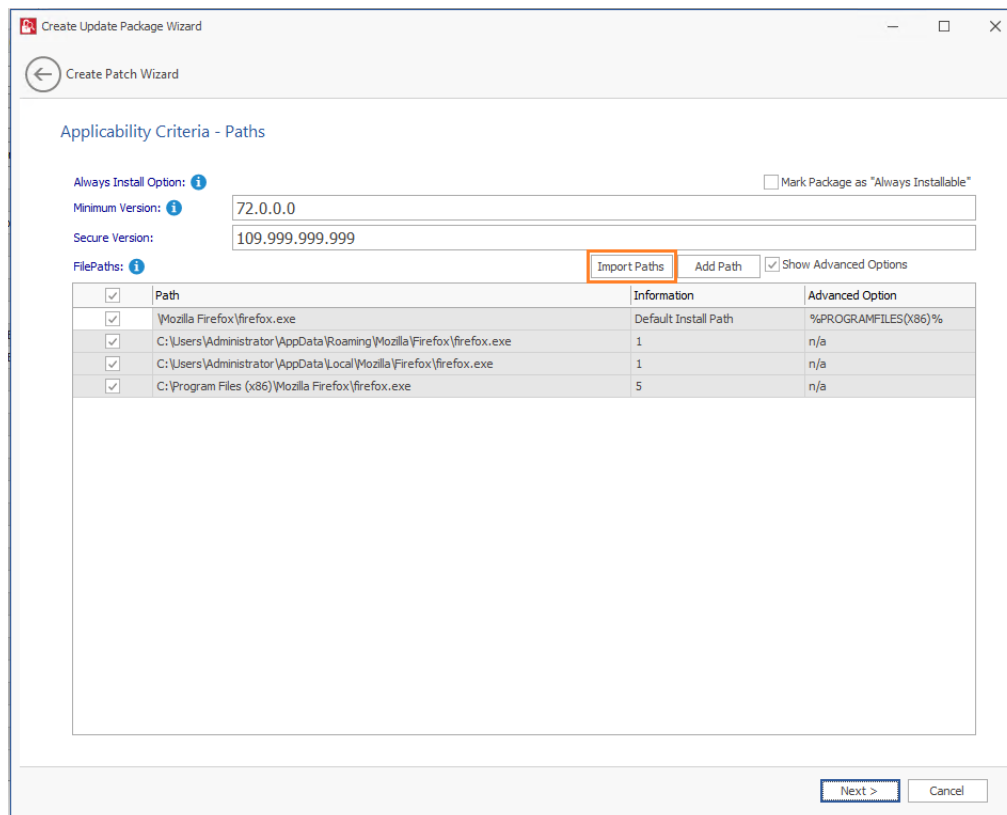
Removed RSAT as a Dependency for Installing SVM Patch Publisher

With this update, you can now install Patch Publisher without the dependency that RSAT should already be installed/enabled on that machine. RSAT will be required to be installed only when you configure a connection to the Windows Server Update Services (WSUS) in the Patch Publisher.

Support for RHEL 9 Scanning

The SVM Single Host Agent v7.6.1.24 (scan agent) now supports scanning of Red Hat Enterprise Linux (RHEL) 9 Operating System.

Search Published Patch by Bulletin ID

In the **SVM Patch Publisher**, when you set a value for **Reference ID** in the **Package Configuration** panel of the **Create Update Package Wizard** and publish a patch to a configured WSUS, the value set for the Reference ID will appear as **Bulletin ID** in the ConfigMgr. This **Bulletin ID** can be used to search the patch in the ConfigMgr.

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

  Refer "New Features and Enhancements" for changelog.

- SVM Daemon v7.6.1.24 (no change)
- SVM System Center Plugin v7.6.1.24 (no change)
- SVM Patch Publisher v7.10.912 (to download, click here)

  Refer "New Features and Enhancements" and "Resolved Issues" 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):

Issue	Description
IOK-1026212	In the Package Content panel, If you add multiple files in "Files to Include" section, only the first file is considering for "Download SPS File".
IOK-1026206	In the BYOP grid, when you click on the Download link, few links fail with a 404 error.

Resolved Issues

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

Issue	Description
IOK-1020732	The version is coming blank if you edit/remove the URL in the Package Contents panel and perform Force Check-In.
IOK-1022403	"Enable WMI" setting is not retaining using web UI.
IOK-753601	Reference ID added in the Package Configuration Panel is not published as Bulletin ID.

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.