

Software Vulnerability Manager (On-Premises Edition) Release Notes

April 2024

Introduction	1
New Features and Enhancements	2
Patch Publisher Enhancements	2
Enabled “Add Local File” Button in Package Contents Panel.....	2
Configured “Restart Service” with “Test and Save Connection”	3
Other Enhancements	3
Software Vulnerability Manager User Interface Enhancements	3
Extended Security Updates (ESUs) Support for End-of-Life Products	4
Dashboard Page Improvements.....	5
Improved Vendor Patch Module Grid and Wizard Performance	5
Marking Windows Operating System as End-of-Life	5
Reference: Latest Binary Versions	5
Known Issues	6
Resolved Issues	6
Community Blogs	7
Product Feedback	7
Legal Information	7

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.

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 (On-Premises Edition) includes the following new features and enhancements:

- [Patch Publisher Enhancements](#)
- [Software Vulnerability Manager User Interface Enhancements](#)
- [Improved Vendor Patch Module Grid and Wizard Performance](#)
- [Marking Windows Operating System as End-of-Life](#)
- [Reference: Latest 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).

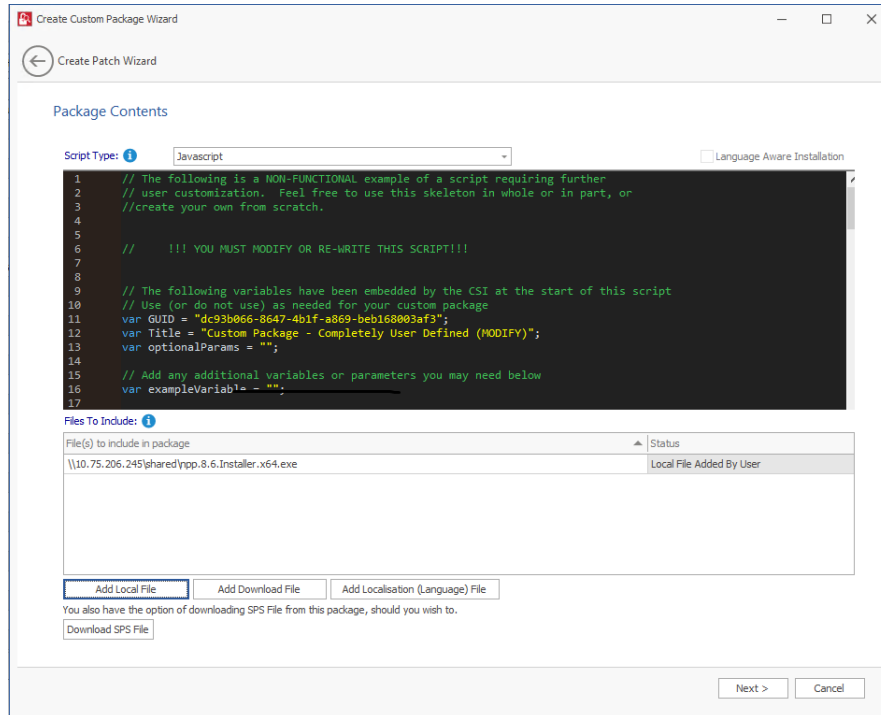
Patch Publisher Enhancements

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

- [Enabled “Add Local File” Button in Package Contents Panel](#)
- [Configured “Restart Service” with “Test and Save Connection”](#)
- [Other Enhancements](#)

Enabled “Add Local File” Button in Package Contents Panel

The **Add Local File** button in the **Package Contents** panel of the **Create Update Package Wizard** is now enabled. By clicking on the **Add Local File** button, you can select the required file that you want to add for the selected path from the local/shared folders. This enhancement allows you to add package files to publish.



Configured “Restart Service” with “Test and Save Connection”

With this update, along with the existing **Restart Service**, the **Test and Save Connection** has been configured to restart Patch Publisher service automatically for the changes to take effect while setting the SVM connection and adding/editing distribution connections. Log messages will be displayed in the Output Window.

Other Enhancements

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

- In the **Create Patch Wizard > Applicability Criteria - Paths** panel, by default **Show Relevant Paths** check box will be selected and displays relevant EOL/Insecure file paths.
- While publishing SPS / VPM patches to Intune deployment system, SVM will select limited paths at a time for the subscription. This enhancement will eliminate the possibility of subscription failure. This is applicable for both Wizard and Subscription.
- The Wizard and Subscription performance for SPS/ VPM patches in the Patch Publisher has been significantly improved because of application optimization.

Software Vulnerability Manager User Interface Enhancements

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

- [Extended Security Updates \(ESUs\) Support for End-of-Life Products](#)

- Dashboard Page Improvements

Extended Security Updates (ESUs) Support for End-of-Life Products

The Extended Security Update (ESU) allows you to override an End-of-Life status to Secure/Insecure for the selected product.

In the Products Smart Groups view, you will be able to add extended support for the End-of-Life Products. Right click on an End-of-Life product for which you wish to add extended support and click on the menu option **Add Extended Support**.

Product Name	Version	SAID	Advisory D.	Criticality	Threat Sc.	CVSS Ba...	Vendor	Insecure	End-Of-Life	Secure	Total	Affected	Download	Product Type
Microsoft ODBC Driver for SQL...	17.10.5.1	SA120152	Microsoft M...	4	4	V3.8	Microsoft	16	0	0	16	8	Download	Program
Microsoft OLE DB Driver for S...	18.6.7	SA120152	Microsoft M...	4	4	V3.8	Microsoft	12	0	0	12	6	Download	Program
Microsoft OLE DB Driver for S...	19.3.2	SA120152	Microsoft M...	4	4	V3.8	Microsoft	2	0	0	2	1	Download	Program
Microsoft SQL Server 2012	KB3194719	SA173550	Microsoft S...	7	7	V2.6	Microsoft	1	0	0	1	1	-	Program
Microsoft SQL Server 2014	KB3194719	SA120152	Microsoft M...	4	4	V3.8	Microsoft	1	0	2	3	3	-	Program
Microsoft SQL Server 2016	-	-	-	-	-	-	Microsoft	0	0	3	3	3	-	Program
Microsoft SQL Server 2022	KB5029379	SA172600	Microsoft S...	16	16	V3.8	Microsoft	1	0	0	1	1	-	Program
Microsoft SQL Server Compact...	-	-	-	-	-	-	Microsoft	0	0	5	5	5	-	Program
Microsoft SQL Server Manage...	-	-	-	-	-	-	Microsoft	0	2	0	2	2	Download	Program
Microsoft SQL Server Manage...	-	-	-	-	-	-	Microsoft	0	4	0	4	4	Download	Program

Enter the date and select the required hosts/sites by clicking on the check box that you want to add for extended support.

Microsoft SQL Server Management Studio 18.x

Extended Security Updates (ESU) Date: 2024-04-30

svm Search

Available Sites		Selected Sites	
<input type="checkbox"/>	Site	<input checked="" type="checkbox"/>	Site
<input checked="" type="checkbox"/>	SVM2019	<input checked="" type="checkbox"/>	SVM2019
<input type="checkbox"/>	SVMTest		

Page 1 of 1

Displaying Available Sites 1 - 2 of 2

Search...

Available Hosts		Selected Hosts	
<input type="checkbox"/>	Site	<input checked="" type="checkbox"/>	Site
<input type="checkbox"/>	SCCM	<input checked="" type="checkbox"/>	SVM2019
<input type="checkbox"/>	FLEXERA		QA_WIN10B
<input type="checkbox"/>	SVMTest		
<input type="checkbox"/>	MacSite		
<input type="checkbox"/>	Active Directory o...		
<input type="checkbox"/>	Active Directory o...		

Save Cancel

Extended support added for the selected product can be seen in the **Scanning > Filter Scan Results > Extended Support**. Right click on the product for which you wish to edit/delete and click on the menu option **Edit Extended Support / Delete Extended Support**.

Dashboard Page Improvements

In the Dashboard page, the **Last Month** column has been introduced to display the last month data information in the following widgets and you can see the count by hovering over the respective bar charts:

- Overview
- Most Prevalent Insecure Software Installations
- Insecure Software Installations weighted Score
- Most Prevalent End-of-Life Software Installations
- Software Overview - Status of Installations
- Criticality Overview - Threat Profile of Vulnerabilities
- Site Overview - Average System Score
- Site Overview - Insecure Software Installations

Improved Vendor Patch Module Grid and Wizard Performance

The load time of the VPM Grid and wizard under the Vendor Patch Module in Patch Publisher/web console has been significantly improved because of application optimization.

Marking Windows Operating System as End-of-Life

With this enhancement, SVM can now differentiate between different Windows Operating System builds and mark them as End-of-Life based on the Operating System build number.

Reference: Latest 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 (no change)
 - SVM Daemon v7.6.1.24 (no change)
 - SVM System Center Plugin v7.6.1.24 (no change)
 - SVM Patch Publisher v7.20.1114 (to download, [click here](#))
- Refer “Patch Publisher Enhancements” 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-1101668	In the SVM console, scheduled export is not working for Extended support grid.

Resolved Issues

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

Issue	Description
IOK-1086983	Patch Publisher service is going to sleep mode.
IOK-1086977	In the Patch Template grid showing a wrong patched version.
IOK-1088052	In the Patch Publisher, VPM packages looping issue.
IOK-1044933	Patch publisher does not use with the newly generated token.
IOK-1077808	Patch publisher is not showing proper error message when token expired.
IOK-1106830	An error appears while publishing a package from the Patch Template.
IOJ-2209294	In Patch Deployment page, Version is appearing as .999.999.999
IOK-1107162	In the Results > Hosts Smart Groups > All Hosts > Showing All Sites drop down, resolved the issue of having limitations to show sites.
IOK-1112339	Unable to view the latest version of the VPM package (Screenpresso).
IOJ-2171317	Marking Windows Operating System Build as End-of-Life.
IOK-1115445	Enhance email validation to accommodate larger top-level domains (TLDs) on Single Sign-On (SSO) screens and User Management.
IOK-1116327	UI issue in User management/Partition Management screen.
IOK-1101186	In Patch Publisher, few packages are failing with VPM subscription due to junk values in silent parameter

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 © 2024 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.