

# Software Vulnerability Manager (On-Premises Edition) Release Notes

December 2023

<b>Introduction .....</b>	<b>1</b>
<b>New Features and Enhancements .....</b>	<b>2</b>
<b>Patch Publisher Enhancements .....</b>	<b>2</b>
Show Relevant Paths Option .....	2
CSIDL Path Enhancement .....	3
Support MSP Packages for Publish .....	4
<b>Software Vulnerability Manager User Interface Enhancements .....</b>	<b>4</b>
Report Configuration Grid Enhancements.....	4
Improved Product Smart Groups Performance.....	5
<b>Reference: Latest Binary Versions.....</b>	<b>5</b>
<b>Resolved Issues.....</b>	<b>6</b>
<b>Community Blogs.....</b>	<b>6</b>
<b>Product Feedback .....</b>	<b>6</b>
<b>Legal Information .....</b>	<b>7</b>

## 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](#)
- [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).

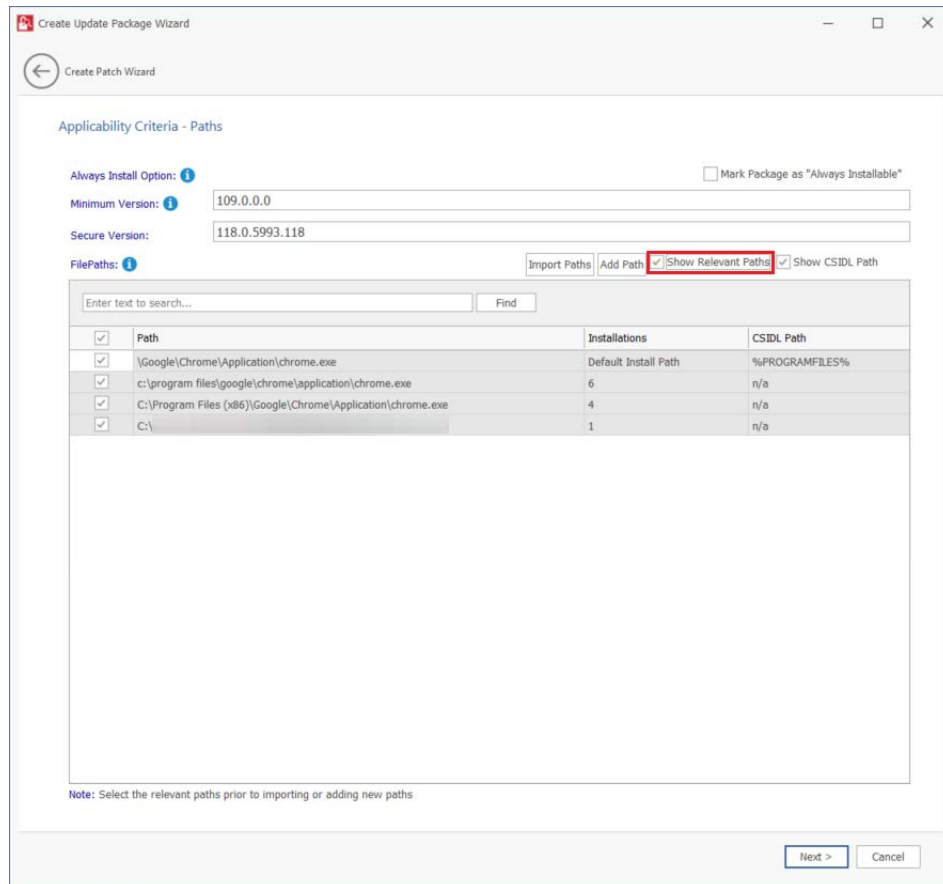
## Patch Publisher Enhancements

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

- [Show Relevant Paths Option](#)
- [Support MSP Packages for Publish](#)
- [CSIDL Path Enhancement](#)

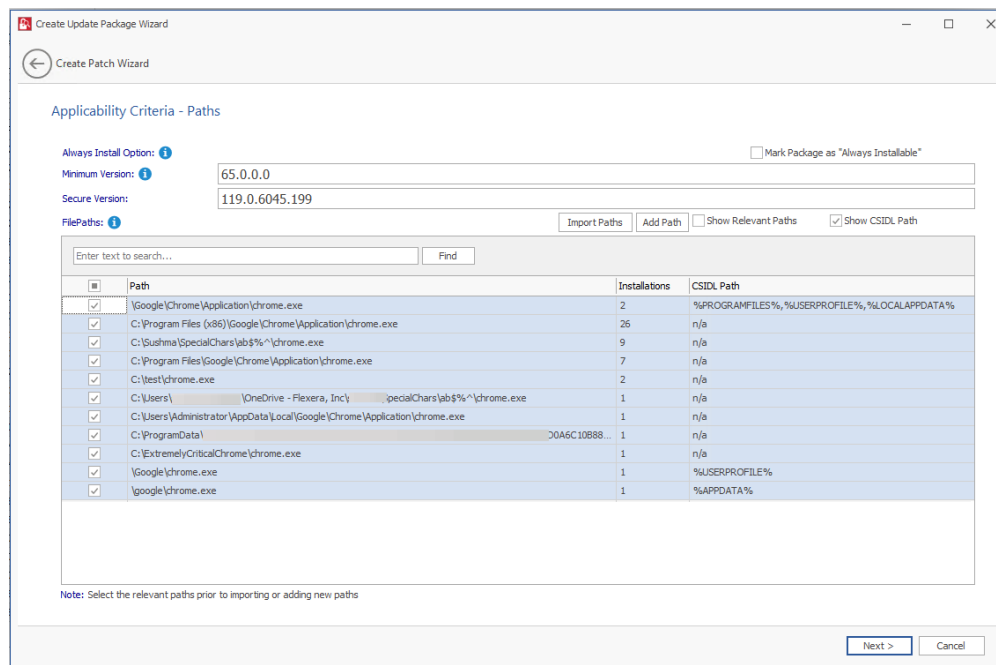
### Show Relevant Paths Option

A new **Show Relevant Paths** check box is introduced in the **Applicability Criteria - Paths** panel of the **Create Update Package Wizard**. All the installations path with a non-zero count in the Installations column are considered as relevant paths. This update provides you with the ability to filter the non-relevant paths. By selecting this check box, only the paths with one or more installations of the selected package will be displayed.



## CSIDL Path Enhancement

In the **Create Update Package Wizard > Applicability Criteria - Paths** panel, previously the applicability criteria: %USERPROFILE%, %APPDATA%, and %LOCALAPPDATA% when used in the **CSIDL Path** column were not working as expected for Microsoft Intune. The issue has been fixed in this update, so the afore mentioned applicability criteria can be used in the **CSIDL Path** column.



## Support MSP Packages for Publish

On the Flexera Package System (SPS) page, along with EXE files, you can now publish and deploy MSP patches to specified end point management systems. To deploy MSP patches, make sure that the parent MSI of the MSP is already installed on the host/device.

## Software Vulnerability Manager User Interface Enhancements

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

- [Report Configuration Grid Enhancements](#)
- [Improved Product Smart Groups Performance](#)

## Report Configuration Grid Enhancements

Following enhancements are added to Reporting > Report Configuration grid:

- **Search by Report Title / Report Format Fields**— You can enter keywords in the **Search by Report Title** search box to find the matching entries in the grid. You can also search for reports either by **Show all Reports** or **Recurring** or **One Time** or **PDF** or **CSV** from the **Reports Format** drop down.

Software Vulnerability Manager

Dashboard

Scanning

Results

Reporting

Report Configuration

Smart Group Notifications

Dashboard

Report Configuration

Generate New Report

Search by Report Title

Report Format

Show all Reports

Report Title

Generate Next Schedule Report...

Nov 28, 2023

Every Month

Oct 28, 2023

Every Month

Nov 20, 2023

Every Month

Nov 15, 2023

Every Month

None (One-Time Report)

31st Aug, 2023 13:05

Recurrence Schedule

Recurring

One Time

PDF

CSV

Every Month

Date Created/Modified

25th Jul, 2023 13:06

30th Aug, 2022 16:28

30th Feb, 2023 16:31

15th Aug, 2023 13:29

31st Aug, 2023 13:27

Last Execution Time

-

-

-

-

-

Report Format

CSV

CSV

CSV

CSV

CSV

File Size

0.02 MB

-

0.01 MB

-

-

Status

Alive

Alive

Alive

Alive

Processed

Download

[Download](#)

[Download](#)

[Download](#)

[Download](#)

[Download](#)

- **Report Format Column**— The **Report Format** column displays the format of the generated report.

Software Vulnerability Manager

Dashboard

Scanning

Results

Reporting

Report Configuration

Smart Group Notifications

Activity Log Notifications

Database Access

Database Console

Database Cleanup

Scheduled Exports

Dashboard

Report Configuration

Generate New Report

Search by Report Title

Search

Report Format: Show all Reports

Report Title	Generate Next Schedule Report	Recurrence Schedule	Last Generation	Date Created/Modified	Last Execution Time	Report Format	File Size	Status	Download
Oct 30, 2023	Every Month	30th Sep, 2023 0...	30th Mar, 2023 12:58	-	CSV	-	Alive	<a href="#">Download</a>	
Oct 30, 2023	None (One-Time Report)	16th May, 2023 11...	16th May, 2023 11:27	0h 0m 2s	CSV	1.19 MB	Processed	<a href="#">Download</a>	
Oct 28, 2023	Every Month	28th Sep, 2023 0...	28th Mar, 2023 18:58	0h 0m 6s	PDF	-	Alive	<a href="#">Download</a>	
Oct 28, 2023	None (One-Time Report)	6th Feb, 2023 17:30	6th Feb, 2023 17:29	0h 0m 1s	PDF	-	Processed	<a href="#">Download</a>	
Nov 20, 2023	Every Month	20th Oct, 2023 05...	25th Jul, 2023 13:04	0h 0m 21s	PDF	2.04 MB	Alive	<a href="#">Download</a>	
Oct 28, 2023	Every Month	28th Sep, 2023 0...	28th Mar, 2023 18:59	0h 0m 6s	PDF	-	Alive	<a href="#">Download</a>	
Oct 28, 2023	Every Month	28th Sep, 2023 0...	28th Mar, 2023 18:55	0h 0m 4s	PDF	-	Alive	<a href="#">Download</a>	
Oct 28, 2023	Every Month	28th Sep, 2023 0...	20th Feb, 2023 17:53	0h 0m 5s	PDF	-	Alive	<a href="#">Download</a>	
-	None (One-Time Report)	25th Oct, 2023 15...	25th Oct, 2023 15:28	-	CSV	0.02 MB	Processed	<a href="#">Download</a>	
Nov 25, 2023	Every Month	25th Oct, 2023 15...	25th Oct, 2023 15:29	-	CSV	0.01 MB	Alive	<a href="#">Download</a>	

- **File Size Column**— The **File Size** column displays the file size of the generated report.

Software Vulnerability Manager

Help

Logout

Dashboard

Scanning

Results

Reporting

Report Configuration

Smart Group Notifications

Activity Log Notifications

Database Access

Database Console

Database Cleanup

Scheduled Exports

Dashboard

Report Configuration

Generate New Report

Search by Report Title

Search

Report Format: Show all Reports

Report Title	Generate Next Schedule Repo...	Recurrence Schedule	Last Generation	Date Created/Modified	Last Execution Time	Report Format	File Size	Status	Download
Oct 30, 2023	Every Month	30th Sep, 2023 0...	30th Mar, 2023 12:58	-	CSV	-	Alive	<a href="#">Download</a>	
Oct 30, 2023	None (One-Time Report)	16th May, 2023 11...	16th May, 2023 11:27	0h 0m 2s	CSV	1.19 MB	Processed	<a href="#">Download</a>	
Oct 28, 2023	Every Month	28th Sep, 2023 0...	28th Mar, 2023 18:58	0h 0m 6s	PDF	-	Alive	<a href="#">Download</a>	
Oct 28, 2023	None (One-Time Report)	6th Feb, 2023 17:30	6th Feb, 2023 17:29	0h 0m 1s	PDF	-	Processed	<a href="#">Download</a>	
Nov 20, 2023	Every Month	20th Oct, 2023 05...	25th Jul, 2023 13:04	0h 0m 21s	PDF	2.04 MB	Alive	<a href="#">Download</a>	
Oct 28, 2023	Every Month	28th Sep, 2023 0...	28th Mar, 2023 18:59	0h 0m 6s	PDF	-	Alive	<a href="#">Download</a>	
Oct 28, 2023	Every Month	28th Sep, 2023 0...	28th Mar, 2023 18:55	0h 0m 4s	PDF	-	Alive	<a href="#">Download</a>	
Oct 28, 2023	Every Month	28th Sep, 2023 0...	20th Feb, 2023 17:53	0h 0m 5s	PDF	-	Alive	<a href="#">Download</a>	
Nov 25, 2023	None (One-Time Report)	25th Oct, 2023 15...	25th Oct, 2023 15:28	-	CSV	0.02 MB	Processed	<a href="#">Download</a>	
Nov 25, 2023	Every Month	25th Oct, 2023 15...	25th Oct, 2023 15:29	-	CSV	0.01 MB	Alive	<a href="#">Download</a>	

- **Last Execution Time Column**— The **Last Execution Time** column displays the number of hours/minutes/seconds of how long it took to generate the report.

Software Vulnerability Manager

Dashboard

Scanning

Results

Report Configuration

Smart Group Notifications

Activity Log Notifications

Database Access

Database Console

Database Cleanup

Scheduled Exports

Dashboard

Report Configuration

Generate New Report

Search by Report Title

Report Format: Show all Reports

Report Title	Generate Next Schedule Report	Recurrence Schedule	Last Generation	Date Created/Modified	Last Execution Time	Report Format	File Size	Status	Download
Oct 30, 2023	Every Month	30th Sep, 2023 0...	30th Mar, 2023 12:58	-	CSV	-	Alive	<a href="#">Download</a>	
Oct 30, 2023	None (One-Time Report)	16th May, 2023 11...	16th May, 2023 11:27	0h 0m 2s	CSV	1.19 MB	Processed	<a href="#">Download</a>	
Oct 28, 2023	Every Month	28th Sep, 2023 0...	28th Mar, 2023 18:58	0h 0m 6s	PDF	-	Alive	<a href="#">Download</a>	
Oct 28, 2023	None (One-Time Report)	6th Feb, 2023 17:30	6th Feb, 2023 17:29	0h 0m 1s	PDF	-	Processed	<a href="#">Download</a>	
Nov 20, 2023	Every Month	20th Oct, 2023 05...	25th Jul, 2023 13:04	0h 0m 21s	PDF	2.04 MB	Alive	<a href="#">Download</a>	
Oct 28, 2023	Every Month	28th Sep, 2023 0...	28th Mar, 2023 18:59	0h 0m 6s	PDF	-	Alive	<a href="#">Download</a>	
Oct 28, 2023	Every Month	28th Sep, 2023 0...	28th Mar, 2023 18:55	0h 0m 4s	PDF	-	Alive	<a href="#">Download</a>	
Oct 28, 2023	Every Month	28th Sep, 2023 0...	20th Feb, 2023 17:53	0h 0m 5s	PDF	-	Alive	<a href="#">Download</a>	
Nov 25, 2023	None (One-Time Report)	25th Oct, 2023 15...	25th Oct, 2023 15:28	-	CSV	0.02 MB	Processed	<a href="#">Download</a>	
Nov 25, 2023	Every Month	25th Oct, 2023 15...	25th Oct, 2023 15:29	-	CSV	0.01 MB	Alive	<a href="#">Download</a>	

## Improved Product Smart Groups Performance

The load time of the smart groups under the Product Smart Groups in the web console has been significantly improved as a result of code and backend optimization.

## 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 v7.18.1101 (to download, [click here](#))  
Refer “Patch Publisher Enhancements” for changelog.
- SVM On-Prem Client Toolkit v5.0.547 (to download, [click here](#)) (no change)

## Resolved Issues

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

Issue	Description
<b>IOK-1072414</b>	While deploying packages to Intune, Subscription was failing due to large number of paths.
<b>IOK-1074137</b>	Due to task API timeout, Patch Publisher not fetching the tasks for large number of devices.
<b>IOK-1072070</b>	From the Patch Publisher UI, service restart is failing for few customers.
<b>IOK-1046547</b>	The WSUS Management Tool is giving an exception when it is relaunched.
<b>IOK-1026212</b>	In the Create Update Package Wizard > Package Contents panel, if we add multiple files only the first file is considered for the Download SPS File.

## 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.