

Software Vulnerability Manager (Cloud Edition) Release Notes

November 2023

Introduction	1
New Features and Enhancements	2
Patch Publisher Enhancements	2
Support MSP Packages for Publish	3
CSIDL Path Enhancement	3
Reference: Latest Binary Versions	3
Resolved Issues	4
Community Blogs	4
Product Feedback	4
Legal Information	5

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, 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 (Cloud Edition) includes the following new features and enhancements:

- [Patch Publisher Enhancements](#)
- [Reference: Latest 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 MSP Packages for Publish](#)
- [CSIDL Path Enhancement](#)

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 specific product is installed on the host/device.

CSIDL Path Enhancement

In the **Create Update Package Wizard > Applicability Criteria - Paths** panel, previously the applicability criteria (%USERPROFILE%, %APPDATA%, and %LOCALAPPDATA%) in the **CSIDL Path** column were not working as expected for Microsoft Intune. With this update, the above mentioned applicability criteria can be used in the **CSIDL Path** column.

Create Update Package Wizard

← Create Patch Wizard

Applicability Criteria - Paths

Always Install Option: ☐ Mark Package as "Always Installable"

Minimum Version: 65.0.0.0

Secure Version: 119.0.6045.199

File Paths: ☐ Show Relevant Paths ☒ Show CSIDL Path

Enter text to search...

Path	Installations	CSIDL Path
[x] Google\Chrome\Application\chrome.exe	2	%PROGRAMFILES%, %USERPROFILE%, %LOCALAPPDATA%
[x] C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	26	n/a
[x] C:\Sushma\SpecialChars\ab\$%^chrome.exe	9	n/a
[x] C:\Program Files\Google\Chrome\Application\chrome.exe	7	n/a
[x] C:\test\chrome.exe	2	n/a
[x] C:\Users\OneDrive - Flexera, Inc\SpecialChars\ab\$%^chrome.exe	1	n/a
[x] C:\Users\Administrator\AppData\Local\Google\Chrome\Application\chrome.exe	1	n/a
[x] C:\ProgramData\00A6C10B88...	1	n/a
[x] C:\ExtremelyCriticalChrome\chrome.exe	1	n/a
[x] \Google\chrome.exe	1	%USERPROFILE%
[x] \google\chrome.exe	1	%APPDATA%

Note: Select the relevant paths prior to importing or adding new paths

Reference: Latest Binary Versions

The following is a list of the latest binary versions available in this release

- SVM ActiveX Plug-in v7.6.0.24 (No change)
- Single Host Agent v7.6.0.24 (No change)
- SVM Daemon v7.6.0.24 (No change)
- SVM System Center Plugin v7.6.0.24 (No change)
- SVM Patch Publisher v7.17.1099 (To download this installer, [click here](#))

Refer [Patch Publisher Enhancements](#) for changelog.

- SVM Cloud Client Toolkit v5.0.561 (To download this installer, [click here](#)). (No change)

This toolkit contains offline utilities such as the Multi-partition Reporting Tool, WSUS Management Tool (also available in SVM Patch Publisher), and Client Data Tool which add value to SVM. This toolkit does not include the Patch Daemon. This toolkit is for SVM Cloud edition only.



Note • *Flexera SVM Patch Configuration* will be deprecated in the future; therefore, you are encouraged to migrate to the new SVM Patch Publisher tool.

Resolved Issues

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

Issue	Description
IOK-1046547	The WSUS Management Tool is giving an exception when it is relaunched.
IOK-1079199	Software Suggestion not working for SVM.

Community Blogs

Please subscribe to the latest posts about Software Vulnerability Manager by going to <https://community.flexera.com/t5/Software-Vulnerability/bg-p/SoftwareVulnerabilityManagementblog> and clicking **Subscribe**.

Please subscribe to the latest release announcements concerning Software Vulnerability Manager by going to <https://community.flexera.com/t5/Software-Vulnerability/bg-p/Software-Vulnerability-Release-blog> and clicking **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.