Software Vulnerability Manager (Cloud Edition) Release Notes

December 2025 - Update 2

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 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, Cinfig Manager, BigFix, or Tanium.

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 publishing 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

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

Support for Config Manager Unified Endpoint Management System

With this update, you can now configure and publish SPS and VPM patches to **Config Manager** Unified Endpoint Management System.

Once the connection to Config Manager is configured, you can use either Patch Automation or Create Patch Wizard to publish SPS and VPM patches to the specified end point management system (Config Manager).

Software Vulnerability Manager User Interface Enhancements

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

Disable Standard Login for Root Accounts When SSO is Configured and Enabled

A new **Disable Standard Login for yourself** check box has been added under **Configuration > Settings > SSO Settings**. When enabled, standard login is blocked for the root account, the password change option is removed from the UI, and if password recovery was previously enabled, the Forgot Password option remains available. If recovery is unavailable or the account becomes locked, users must raise a support ticket. This feature is controlled by a separate flag visible only to root users and applies only if opted in, ensuring it does not affect other customers unless they enable it. When enabling, the system prompts for confirmation and informs that a temporary password will be sent to the configured email. This ensures secure access when switching from SSO to standard login.

New “API Access” Permission in User Management

A new **API Access** option has been introduced under **User Management > Create New User** within the **User Roles & Permissions** section. This option is available when assigning **Read/Write** permissions. Selecting API Access grants the user API-level capabilities; however, enabling this option will disable standard API access for the account to ensure controlled and secure integration. Administrators can configure this alongside other roles such as Scanning, Reporting, and Patching, providing granular control over user permissions.

Reference: Latest Binary Versions

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

- SVM ActiveX Plug-in v7.6.0.29 (No change)
- Single Host Agent v7.6.0.29 (No change)
- SVM Daemon v7.6.0.29 (No change)
- SVM System Center Plugin v7.6.0.29 (No change)
- SVM Patch Publisher v7.29.2153 (To download this installer, click here)

  Refer “Enhancements” for changelog.
- SVM Cloud Client Toolkit v5.0.1926 (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 *• On September 23, 2024, digital signing updates were released for SVM Patch Publisher (version 7.22.1546) and SVM Cloud Client Toolkit (version 5.0.1546).*

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

Known Issues

The following table lists the known issues in Software Vulnerability Manager (Cloud Edition):

Issue	Description
IOK-1896655	For ConfigMgr, the Windows authenticated connection, throwing error at the time of selecting connection.
IOK-1905092	For ConfigMgr, Create Custom Package and Agent Deployment is failing to save wizard data.

Issue	Description
IOK-1905126	For ConfigMgr, uninstalaltion is not working.

Resolved Issues

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

Issue	Description
IOK-1860456	In the Package Feed Module, few applications are unable to download.

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

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.