Software Vulnerability Manager (Cloud Edition) Release Notes

July 2025

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, 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:

- Enhanced Security Check for Unsigned VPM Package Deployment
- Expanded Package Support in Vendor Patch Module (VPM)

- Reference: Latest Binary Versions

Enhanced Security Check for Unsigned VPM Package Deployment

In Patch Publisher, a new security warning pop-up has been introduced for VPM patches when **Create Update Package** for unsigned applications. Users must confirm their intent before proceeding. Digitally signed packages are not affected and continue through the standard deployment process without any prompt.

Expanded Package Support in Vendor Patch Module (VPM)

The Vendor Patch Module (VPM) has been significantly enhanced with the addition of approximately 1500 new packages, increasing the total package coverage from 8800 to 10300 approximately. This expansion provides broader application support within both the SVM UI and Patch Publisher, enabling users to benefit from a more comprehensive and diverse patching library while continuing to leverage the same streamlined automation and deployment workflows. In future, more packages will be added to further enrich the VPM coverage.

***Note** • To leverage the expanded VPM Library, the new version of Patch Publisher (v7.27.1964) is required.*

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 v7.27.1964 (To download this installer, click here)

  Refer “Enhancements” for changelog.
- SVM Cloud Client Toolkit v5.0.1926 (To download this installer, click here)

  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.*

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.