Software Vulnerability Manager (On-Premises Edition) Release Notes

July 2025

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

- Patch Publisher Enhancements
- Software Vulnerability Manager User Interface Enhancements
- Expanded Package Support in Vendor Patch Module (VPM)
- 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.

- Introduced New SVM Connection Status Indicators
- Migration from ADAL to MSAL for Microsoft Intune Integration
- Enhanced Security Check for Unsigned VPM Package Deployment

Introduced New SVM Connection Status Indicators

Previously, when opening Patch Publisher, there was no clear visual indication of whether the SVM connection exists or not. With the introduction of connection status icons, users now have clear visibility into the current state of the SVM connection at a glance.

- **Green Icon—**Displayed when the SVM connection is active.
- **Red Icon—**Displayed when the SVM connection is inactive or not yet configured.

This enhancement improves the overall user experience during SVM configuration, reduces confusion, and improves transparency.

Migration from ADAL to MSAL for Microsoft Intune Integration

The SVM Patch Publisher have migrated from Azure Active Directory Authentication Library (ADAL) to Microsoft Authentication Library (MSAL). The update enhances security, ensures compliance with Microsoft's latest standards, and supports advanced authentication scenarios through modern identity frameworks.

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.

Software Vulnerability Manager User Interface Enhancements

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

- Introduced New “Alerts” Menu in the SVM UI

Introduced New “Alerts” Menu in the SVM UI

A new **Alert** menu has been added to the top-right corner of the Software Vulnerability Manager user interface, providing users with timely notifications.

With this update, the **Alert** menu displays key information such as:

- **VT Sync details—**Displays the last sync details.
- **Latest Build details—**Displays notification about newly available build.

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 version of the binaries provided are:

- SVM ActiveX Plug-in v7.6.1.29 (No change)
- Single Host Agent v7.6.1.29 (No change)
- SVM Daemon v7.6.1.29 (No change)
- SVM System Center Plugin v7.6.1.29 (No change)
- SVM Patch Publisher v7.27.1964 (to download, click here)

Refer “Patch Publisher Enhancements” for changelog.

Note • *Customers using Workspace One can skip this Patch Publisher release.*

- SVM On-Prem Client Toolkit v5.0.1926 (to download, click here)

Note • *On September 23, 2024, digital signing updates were released for SVM Patch Publisher (version 7.22.1546) and SVM On-Prem Client Toolkit (version 5.0.1546).*

Resolved Issues

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

Issue	Description
IOK-1355538	Firefox VPM-Subscribed Package Installation Failed in Patch Publisher.

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 any suggestions 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

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.