Software Vulnerability Manager (On-Premises Edition) Release Notes

March 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
- 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.

- Hide Deployment Notifications in Workspace ONE
- Paginated Intune Groups

Hide Deployment Notifications in Workspace ONE

A new **Hide Notification** check box has been introduced when adding connections to Workspace ONE. This enhancement allows users to control the visibility of notifications, reducing unnecessary alerts, and ensuring a streamlined user experience.

Paginated Intune Groups

In the **Intune Assignment Groups** dialog box, pagination has been enhanced with the addition of the **Next** and **Previous** buttons, improving navigation between pages.

- **Next Button—** Click to proceed to the next page.
- **Previous Button—** Click to return to the previous page.

Software Vulnerability Manager User Interface Enhancements

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

- Manage Assignments in Quick Patch

- Paginated Intune Groups

Manage Assignments in Quick Patch

The **Manage Assignments** panel has been introduced in QuickPatch, enhancing the management of endpoint deployments during Intune publishing. This new panel allows users to assign deployments within the endpoint management system.

In this panel, you can add the following assignments during endpoint deployments in Intune publishing:

- **Add Groups—** Assigns specific groups
- **Add All Devices—** Assigns all devices
- **Add All Users—** Assigns all users

These assignments can be applied to the **Required**, **Available**, and **Uninstall** sections.

Paginated Intune Groups

In the **Manage Assignments** option of **QuickPatch**, **Subscription**, and **Patch Deployment Status** pages, the **Intune Assignment Groups** dialog box now includes improved pagination with scrolling. As you scroll, the next set of data loads, improving usability and navigation.

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 v7.25.1926 (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).*

Known Issues

The following table lists the known issues in Software Vulnerability Manager (On-Premises Edition):

Issue	Description
IOK-1345425	In the SVM UI, the Deselect option is not available in the Add Groups pop-up for Intune connections.

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-1337474	In Patch Publisher version 7.24, if only one WSUS connection is added as a distribution system and no groups are selected for deployment, the approval task encounters an “Object reference not set to an instance of an object” error.
IOK-1060172	The Client Data Tool returns an Invalid Token error when the password includes special characters.
IOK-1343745	For certain users, the minimum version for Firefox (x64) is not displaying correctly in the VPM subscription.
IOK-1341890	In SVM Virtual Appliance, configuring a manual IP results in a connection failure during login.
IOK-1320811	The Automatic Virtual Appliance upgrade is failing for RPM version 7.6.1.31

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

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.