Software Vulnerability Manager (On-Premises Edition) Release Notes

September 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

- Multi-Setup Package Support in Vendor Patch Module (VPM)
- Reference: Latest OnPrem Builds
- Reference: Latest Binary Versions

Multi-Setup Package Support in Vendor Patch Module (VPM)

The Vendor Patch Module (VPM) now supports publishing and deploying multiple setup files within a single package to the Intune portal, simplifying multi-setup application delivery. This enhancement resolves deployment readiness issues, enables successful installations, and extends support across **SVM** and **Patch Publisher**. These setup files are now visible in the **Patch Information** dialog box, giving improved visibility and control over deployments.

Reference: Latest OnPrem Builds

The following build versions are available:

- RPM Builds
  - **RHEL 8—** csi-7.6.1.34-0.el8.x86_64.php7.rpm
  - **RHEL 9—** csi-7.6.1.34-0.el9.x86_64.php8.rpm
- Oracle Linux 9 Virtual Appliance for VMware, Hyper-V, and Red Hat OpenShift (No change)
  - svm-appliance-7.6.1.30-570f28b-hyperv.zip (To update, follow the Software Updates process)
  - svm--appliance-7.6.1.30-570f28b.ova (To update, follow the Software Updates process)

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—** v7.28.2019 (to download, click here)

  Refer "Enhancements" for changelog.
- **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).*

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

Copyright © 2025 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.