Software Vulnerability Manager (On-Premises Edition) Release Notes

January 2026

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

Patch Publisher Enhancements

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

- Support for Config Manager Unified Endpoint Management System

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
- New “API Access” Permission in User Management
- Integrating Intune Publish with SVM Cloud
- Package Creation Wizard in Vendor Patch Module (for MSI packages)

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.

Integrating Intune Publish with SVM Cloud

This feature is available for **MSI** packages in **Vendor Patch Module (VPM)** patches. Upcoming release will expand the feature to EXE packages.

Patch publishing functionality is now integrated into SVM Cloud, allowing patches to be published directly to Intune. To support this capability, a new **Cloud** section has been added under **Patching > Distribution System Connections** in the SVM Cloud interface, where you can configure your Intune connection details. This integration streamlines the workflow by enabling patch publishing directly from SVM Cloud.

Package Creation Wizard in Vendor Patch Module (for MSI packages)

This feature is available for **MSI** packages in **Vendor Patch Module (VPM)** patches in the SVM console.

New wizard pages have been introduced to streamline MSI packages in the Vendor Patch Module patches. This enhancement provides guided steps for configuring update packages, including customization options to publish patches to more than one endpoint management system at the same time.

To do so, right-click the MSI package in the VPM and select Create Update Package. Complete the process by following the steps provided.

Enhanced Patch Publisher and AdminStudio Integration

With this update, SVM packages are automatically assigned to a default AdminStudio workflow (Import + Customization) and marked as *Subscribed* for automation. You can also place non-VPM packages in a monitored shared directory for scheduled import. After configuring AdminStudio REST access and the shared path, Patch Publisher via automation or the wizard can seamlessly stream both VPM and non-VPM packages into AdminStudio for repackaging and distribution with minimal manual effort.

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—** v7.29.2188 (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).*

Known Issues

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

Issue	Description
IOK-1896655	For ConfigMgr, the Windows authenticated connection, throwing error at the time of selecting connection.
IOK-1929114	In Patch Publisher, the **Import Paths** section in **Step 3 (Applicability Criteria – Paths panel)** of the *Create Update Packages for VPM patches* workflow is not functioning as expected.

Issue	Description
IOK-1929173	In Patch Publisher, **Step 3 (Applicability Criteria – Paths panel)** of the *Create Update Packages for VPM patches* workflow is not functioning as expected when evaluating **Detection** for the uninstall action in Configuration Manager.

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-1860456	In the Package Feed Module, few applications are unable to download.
IOJ-2198861	An error message appears when editing and saving the Network Appliance Agent configuration in the SVM UI.
IOK-1861058	Typo in the SVM UI grid.
IOK-1871299	Smart Group notifications not working.
IOK-1347437	Fixed Microsoft Teams version showing incorrectly on Scan Results.

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

Restricted Rights Legend