Software Vulnerability Manager (Cloud Edition) Release Notes

June 2022

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 an 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 or VMware® Workspace One.

New Features and Enhancements

Software Vulnerability Manager (Cloud Edition) includes the following new features and enhancements:

- SVM Patch Publisher Enhancements
- Binary Versions

Note • To see the following new features and enhancements in your Software Vulnerability Manager (Cloud Edition) interface, you must refresh your browser's cache (press Ctrl+F5).

SVM Patch Publisher Enhancements

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

- Agent Deployment View
- Patch Template View
- Create Custom Package for Bring Your Own Patch (BYOP)
- Flexera Package System (SPS) View Enhancements
- Configure View in the Vendor Patch Module

Agent Deployment View

Agent Deployment view gives summary of the Software Vulnerability Manager agents currently installed on the endpoints in the network. You can also create and publish the agent to the configured endpoint management system for deployment.
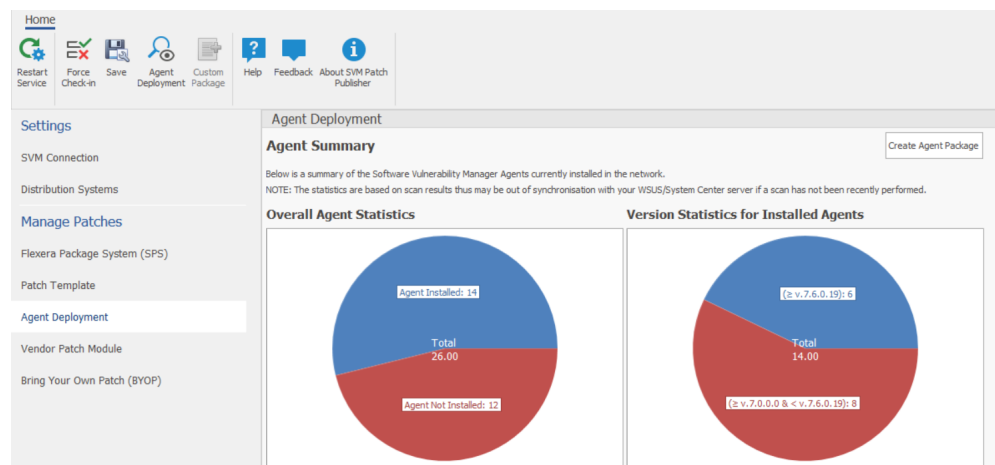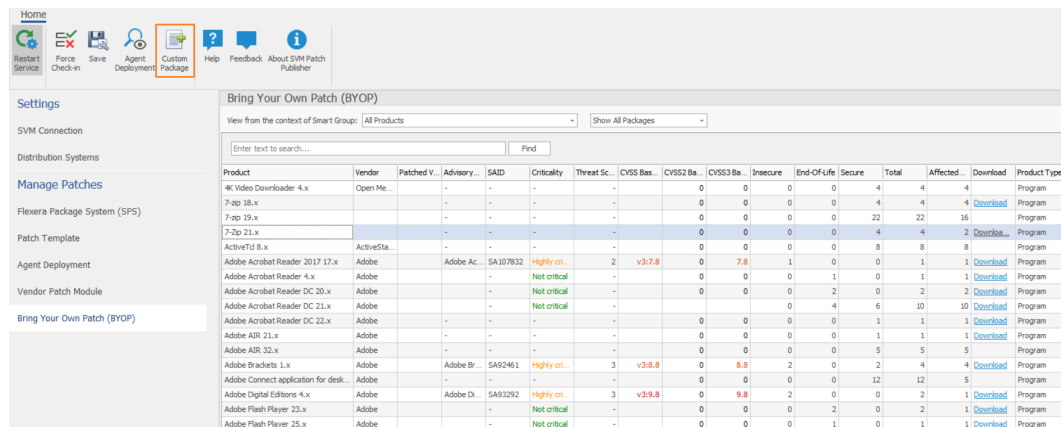

For more information, see Agent Deployment.

Patch Template View

The Patch Template view displays the SPS patches that are saved as Patch Templates. This view also enables you to edit and publish templates to one of the configured endpoint management systems.

Create Custom Package for Bring Your Own Patch (BYOP)

A new button by the name **Custom Package** is introduced in the ribbon to create and publish custom packages. The button gets enabled for the Flexera Package System (SPS) and Bring Your Own Patch (BYOP) views.

Flexera Package System (SPS) View Enhancements

The following improvements have been added in the Flexera Package System (SPS) View.

- Create Uninstall Package
- Create Custom Package
- Package Contents Panel
- Applicability Criteria - Paths Panel

Create Uninstall Package

Products that are listed as **Yes** in the **Uninstallable** column are eligible for creating an uninstall package. To create uninstall package, right-click and select the **Create Uninstall Package** from the context menu.

Create Custom Package

With this update, you can create a new custom package for SPS patches. While creating a custom package, you need to add a download file link and then update the script in the Package Content panel. To create a custom package, right-click and select the **Create Custom Package** from the context menu.

Package Contents Panel

With this update, you will be able to change the files that are included in the SPS package and add localization (language) file to the SPS package.

Applicability Criteria - Paths Panel

In the Applicability Criteria - Paths Panel, you can now specify a path and CSDIL values for a package
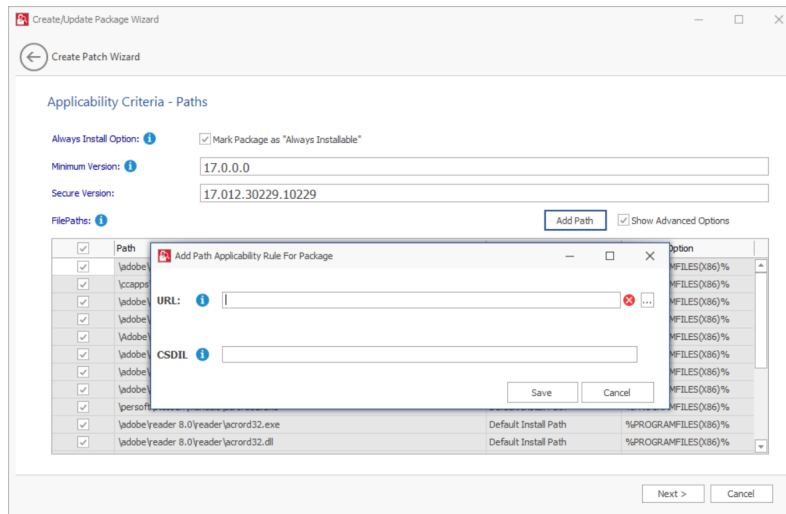
Configure View in the Vendor Patch Module

With this update, you can configure the Vendor Patch Module view to display the patches based on the criteria selected in the Configure View dialog.
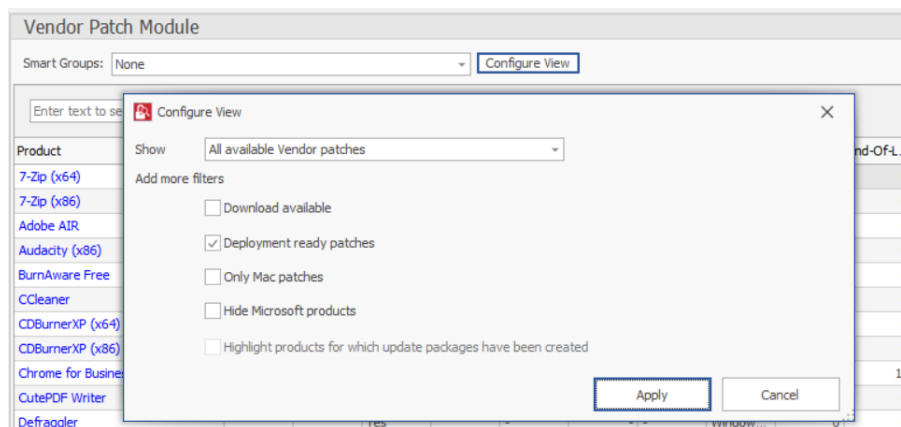
Binary Versions

The following version of the binaries provided are:

● SVM ActiveX Plug-in v7.6.0.19 (no change)

● Single Host Agent v7.6.0.19 (no change)

● SVM Daemon v7.6.0.19 (no change)

● SVM System Center Plugin v7.6.0.19 (no change)

● SVM Patch Publisher v7.1 (to download, click here)

● SVM Cloud Client Toolkit v5.0.561 (to download, click here) (no change)

This toolkit contains offline utilities such as the Multi-partition Reporting Tool, WSUS Management Tool and Client Data Tool which add value to SVM. This toolkit does not consist of Patch Daemon. This toolkit is for SVM Cloud edition only.

Patch Daemon will be deprecated in the future; therefore, you are encouraged to migrate to the new SVM Patch Publisher tool.

- SVM On-Prem Client Toolkit v5.0.547 (to download, click here) (no change)

This toolkit contains Patch Daemon and offline utilities such as the Multi-partition Reporting Tool, WSUS Management Tool and Client Data Tool which add value to SVM.

Known Issues

The following table lists the known issues in Software Vulnerability Manager (Cloud Edition):

Issue	Description
IOK-704176	When connection to Intune is established for the first time with an App Category, publishing of SPS and VPM patches to this Intune connection will fail. Please follow the below steps for the workaround: • Delete the configured App Category and save the Intune connection. • Publish at least one patch to the Intune connection without App Category. • Reconfigure the Intune connection with the App Category. Now all patch publishes to Intune should work.

Resolved Issues

The following table lists the customer issues that were resolved in Software Vulnerability Manager (Cloud Edition):

Issue	Description
IOK-707192	Changed API "action=get_host_scan_results" from "POST" to "GET". For more information, see List Scan Result for Each Host.
IOK-706801	In Advisory smart groups, when click on Host or Products or Installations "NO DATA" message will appear.

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 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

Restricted Rights Legend