# Software Vulnerability Manager (Cloud Edition) Release Notes

March 2023

# 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, VMware® Workspace One, or BigFix.

# New Features and Enhancements

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

- Patch Publisher Enhancements

- Removed RSAT as a Dependency for Installing SVM Patch Publisher

- Search Published Patch by Bulletin ID

- 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).*

## Patch Publisher Enhancements

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

- Vendor Patch Module (VPM) View Enhancements

- "Download" Column in Bring Your Own Patch (BYOP) View

- Download SPS File Option

## Vendor Patch Module (VPM) View Enhancements

Following enhancements are added to Vendor Patch Module (VPM) view:

- **Download Column—** The new **Download** column has been added in the VPM grid. Clicking on the **Download** link will downloaded the patch.



- **Highlighting Deployed Patches—** The patches that are published to a configured endpoint management system will be displayed in green color.

- **Enhanced Patch Information—** The Patch Information dialog box now displays the entire Silent and Uninstall parameters.



# "Download" Column in Bring Your Own Patch (BYOP) View

A new **Download** column has been added to the BYOP grid. Clicking on the **Download** link will download the patch.

.

# Download SPS File Option

A new **Download SPS File** button is introduced in the **Package Contents** panel of the **Create Update Package Wizard**, to download the SPS file for the patch that is being published. By clicking on the button, the SPS file for the patch will be downloaded. Upon downloading the SPS file, the file path link will be displayed in the **SPS File Location** field.

# Removed RSAT as a Dependency for Installing SVM Patch Publisher

With this update, you can now install Patch Publisher without the dependency that RSAT should already be installed/enabled on that machine. RSAT will be required to be installed only when you configure a connection to the Windows Server Update Services (WSUS) in the Patch Publisher.

# Search Published Patch by Bulletin ID

In the **SVM Patch Publisher**, when you set a value for **Reference ID** in the **Package Configuration** panel of the **Create Update Package Wizard** and publish a patch to a configured WSUS, the value set for the Reference ID will appear as **Bulletin ID** in the ConfigMgr. This **Bulletin ID** can be used to search the patch in the ConfigMgr.

# Binary Versions

The following version of the binaries provided are:

- SVM ActiveX Plug-in v7.6.0.24 (no change)

- Single Host Agent v7.6.0.24 (no change)

- SVM Daemon v7.6.0.24 (no change)

- SVM System Center Plugin v7.6.0.24 (no change)

- SVM Patch Publisher v7.9.906 (to download, click here)

  Refer "New Features and Enhancements" for changelog.

- 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.

---

***Note •*** *The Flexera SVM Patch Configuration will be deprecated in the future; therefore, you are encouraged to migrate to the new SVM Patch Publisher tool.*

# Known Issues

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

| Issue | Description |
| --- | --- |
| IOK-1026212 | In the Package Content panel, If you add multiple files in "Files to Include" section, only the first file is considering for "Download SPS File". |
| IOK-1026206 | In the BYOP grid, when you click on the Download link, links fail with a 404 error. |

# Resolved Issues

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

| Issue | Description |
| --- | --- |
| IOK-1020732 | The version is coming blank if you edit/remove the URL in the Package Contents panel and perform Force Check-In. |
| IOK-1022403 | "Enable WMI" setting is not retaining using web UI. |
| IOK-753601 | Reference ID added in the Package Configuration Panel is not published as Bulletin ID. |

# 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

Copyright © 2023 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.