

# Software Vulnerability Manager (On-Premises Edition) Release Notes

June 2022

<b>Introduction</b> .....	<b>1</b>
<b>New Features and Enhancements</b> .....	<b>2</b>
<b>Enhanced SVM Patch Publisher</b> .....	<b>2</b>
Create and Publish Flexera Package System (SPS), Agent, and Vendor Patch Module (VPM) Patches .....	2
Support for BigFix Unified Endpoint Management System .....	2
<b>Host Deletion Settings</b> .....	<b>3</b>
<b>Improved Content of Smart Groups Notification</b> .....	<b>3</b>
<b>Binary Versions Changed</b> .....	<b>3</b>
<b>Known Issues</b> .....	<b>4</b>
<b>Resolved Issues</b> .....	<b>4</b>
<b>Community Blogs</b> .....	<b>4</b>
<b>Product Feedback</b> .....	<b>4</b>
<b>Legal Information</b> .....	<b>5</b>

## 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.

# New Features and Enhancements

Software Vulnerability Manager (On-Premises Edition) includes the following new features and enhancements:

- [Enhanced SVM Patch Publisher](#)
- [Host Deletion Settings](#)
- [Improved Content of Smart Groups Notification](#)
- [Binary Versions Changed](#)



---

**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).

## Enhanced SVM Patch Publisher

SVM Patch Publisher is enhanced with the following new features:

- [Create and Publish Flexera Package System \(SPS\), Agent, and Vendor Patch Module \(VPM\) Patches](#)
- [Support for BigFix Unified Endpoint Management System](#)

## Create and Publish Flexera Package System (SPS), Agent, and Vendor Patch Module (VPM) Patches

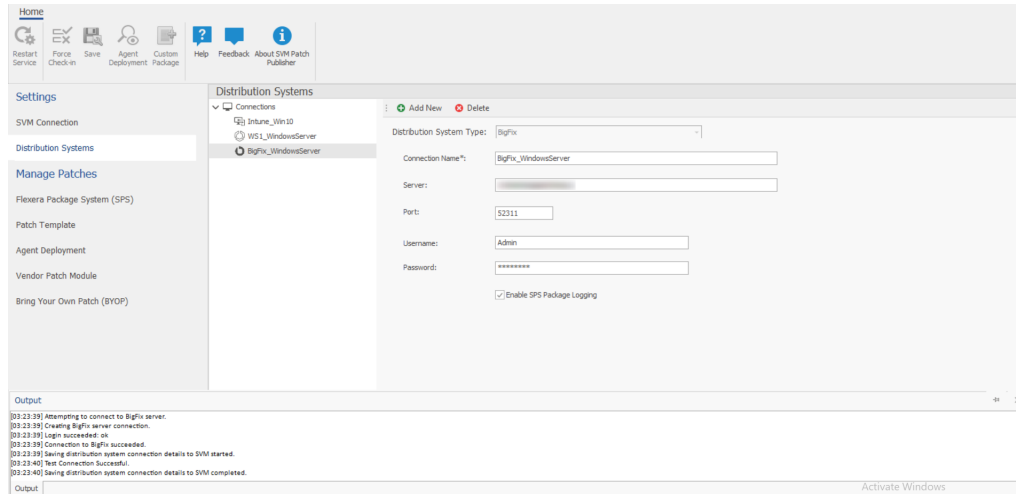
The Manage Patches view is enabled in this update with the following menu:

- **Flexera Package System (SPS)**—View, create and publish SPS patches to the configured endpoint management systems.
- **Patch Template**—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.
- **Agent Deployment**—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.
- **Vendor Patch Module**—View, create and publish VPM patches to the configured endpoint management systems.
- **Bring Your Own Patch (BYOP)**—Identify applications that not covered by SPS and VPM patch catalogs to bring your own patch. You can create and publish custom packages.

For more details, see [Manage Patches](#).

## Support for BigFix Unified Endpoint Management System

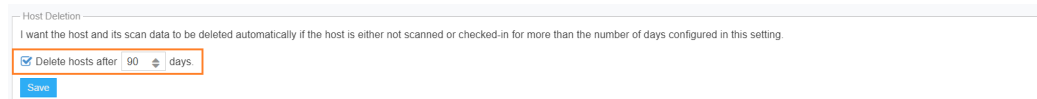
Configure and publish SPS and VPM patches to BigFix Unified Endpoint Management System.



Once the connection to BigFix is configured, you can use either Patch Automation or ActiveX to publish SPS and VPM patches to the specified end point management system (BigFix).

## Host Deletion Settings

A new setting to delete hosts and their scan data for which the last scanned/check-in time is greater than the specified number of days.



## Improved Content of Smart Groups Notification

With this update, you will see more detailed information in smart group notification email. If any advisory changes for advisory smart group, details such as creation date, criticality, CVSS score will be included in the email notification.

## Binary Versions Changed

The following version of the binaries provided are:

- SVM ActiveX Plug-in v7.6.1.19 (no change)
- Single Host Agent v7.6.1.19 (no change)
- SVM Daemon v7.6.1.19 (no change)
- SVM System Center Plugin v7.6.1.19 (no change)
- SVM Patch Publisher v7.1 (to download, [click here](#))
- SVM On-Prem Client Toolkit v5.0.547 (to download, [click here](#)) (no change)

# Known Issues

This release of Software Vulnerability Manager (On-Premises Edition) does not include any known issues. Software Vulnerability Manager (On-Premises Edition):

Issue	Description
<b>IOK-704176</b>	<p>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:</p> <ul style="list-style-type: none"><li>• Delete the configured App Category and save the Intune connection.</li><li>• Publish at least one patch to the Intune connection without App Category.</li><li>• Reconfigure the Intune connection with the App Category.</li></ul> <p>Now all patch publishes to Intune should work.</p>

# Resolved Issues

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

Issue	Description
<b>IOK-706801</b>	In Advisory smart groups, when click on Host or Products or Installations “NO DATA” message will appear.
<b>IOJ-2217368</b>	Smart group notifications not working for certain Advisory configuration.
<b>IOJ-2250444</b>	Enhanced Intune Assignment Groups to display all data in SVM Patch Publisher.

# 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 © 2022 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.