

# Software Vulnerability Manager (Cloud Edition) Release Notes

June 2022

<b>Introduction .....</b>	<b>1</b>
<b>New Features and Enhancements .....</b>	<b>2</b>
<b>SVM Patch Publisher Enhancements .....</b>	<b>2</b>
Agent Deployment View .....	2
Patch Template View .....	3
Create Custom Package for Bring Your Own Patch (BYOP).....	3
Flexera Package System (SPS) View Enhancements .....	3
Create Uninstall Package .....	3
Create Custom Package .....	4
Package Contents Panel .....	4
Applicability Criteria - Paths Panel .....	4
Configure View in the Vendor Patch Module.....	5
<b>Binary Versions .....</b>	<b>5</b>
<b>Known Issues .....</b>	<b>6</b>
<b>Resolved Issues.....</b>	<b>6</b>
<b>Community Blogs .....</b>	<b>6</b>
<b>Product Feedback .....</b>	<b>7</b>
<b>Legal Information .....</b>	<b>8</b>

## 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).

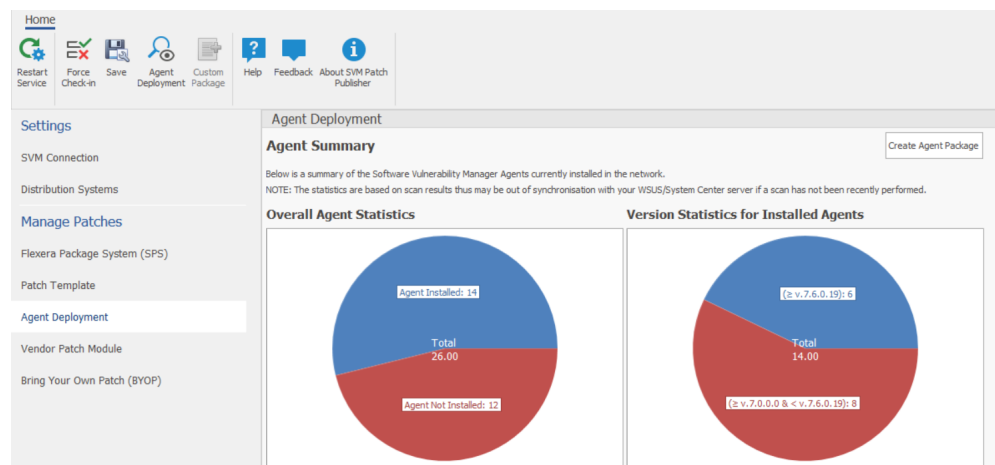
## SVM Patch Publisher Enhancements

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.



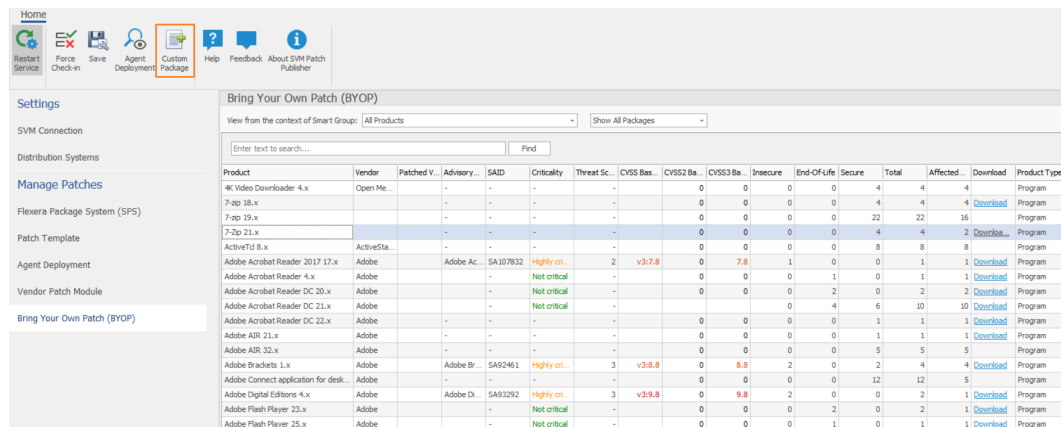
For more information, see [Agent Deployment](#).

## 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.



Product	Vendor	Patched Y...	Advisory...	SAID	Criticality	Threat Sc...	CVSS Bas...	CVSS2 Ba...	CVSS3 Ba...	Insecure	End-Of-Life	Secure	Total	Affected	Download	Product Type
4K Video Downloader 4.x	Open Me...	-	-	-	-	-	-	0	0	0	0	4	4	4	Download	Program
7-zip 18.x	-	-	-	-	-	-	-	0	0	0	0	4	4	4	Download	Program
7-zip 19.x	-	-	-	-	-	-	-	0	0	0	0	22	22	16	Download	Program
7-Zip 21.x	-	-	-	-	-	-	-	0	0	0	0	4	4	2	Download	Program
ActiveTcl 8.x	ActiveSta...	-	-	-	-	-	-	0	0	0	0	8	8	8	Download	Program
Adobe Acrobat Reader 2017 17.x	Adobe	-	-	SA107832	Highly cr...	2	v3:7.8	0	7.8	1	0	0	1	1	Download	Program
Adobe Acrobat Reader 4.x	Adobe	-	-	-	Not critical	-	-	0	0	0	1	0	1	1	Download	Program
Adobe Acrobat Reader DC 20.x	Adobe	-	-	-	Not critical	-	-	0	0	0	2	0	2	2	Download	Program
Adobe Acrobat Reader DC 21.x	Adobe	-	-	-	Not critical	-	-	-	-	0	4	6	10	10	Download	Program
Adobe Acrobat Reader DC 22.x	Adobe	-	-	-	-	-	-	0	0	0	0	1	1	1	Download	Program
Adobe AIR 21.x	Adobe	-	-	-	-	-	-	0	0	0	0	1	1	1	Download	Program
Adobe AIR 32.x	Adobe	-	-	-	-	-	-	0	0	0	0	5	5	5	Download	Program
Adobe Brackets 1.x	Adobe	-	-	SA92461	Highly cr...	3	v3:8.8	0	8.8	2	0	2	4	4	Download	Program
Adobe Connect application for desk...	Adobe	-	-	-	-	-	-	0	0	0	0	12	12	5	Download	Program
Adobe Digital Editions 4.x	Adobe	-	-	SA93292	Highly cr...	3	v3:9.8	0	9.8	2	0	0	2	1	Download	Program
Adobe Flash Player 23.x	Adobe	-	-	-	Not critical	-	-	0	0	0	2	0	2	1	Download	Program
Adobe Flash Player 25.x	Adobe	-	-	-	Not critical	-	-	0	0	0	1	0	1	1	Download	Program

## 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.

Flexera Package System (SPS)

Smart Groups: All Products

Configure View

Enter text to search...

Find

Product	Patched Versi...	Vendor	Architecture	SAID	Criticality	Threat Score	Detected	Advisory Publ...	Insecure	End-Of-Life	Secure	Total	Hosts	Uninstallable
UltraVNC 1.x	1.0.9.1		Windows 64...	SA41208	Moderately	-	10th March...	30th August...	2	0	0	0	2	1
Adobe Brack...	1.14.1	Adobe	Windows 32...	SA92461	Highly Critical	3	24th April, 2...	10th Decemb...	2	0	0	0	2	2
Adobe Acrobat...	17.012.30229	Adobe	Windows 32...	SA107832	Highly Critical	2	15th June, 2...	12th April, 2...	1	0	0	0	1	1
Adobe Reader	22.x (Contin...	Adobe	Windows 32...	SA107832	Highly Critical	2	27th June, 2...	12th April, 2...	0	9	0	0	9	9
Amazon Corr...	8.332.08.1	Amazon.com	Windows 32...	SA107975	Moderately	6	15th Septem...	19th April, 2...	7	0	0	0	7	3
Amazon Corr...	8.332.08.1	Amazon.com	Windows 64...	SA107975	Moderately	6	23rd April, 2...	19th April, 2...	23	0	0	0	23	9
FileZilla FTP...	3.48.0		Windows 64...	SA94916	Moderately	-	03rd June, 2...	29th April, 2...	1	0	0	0	1	1
Mozilla Fi...	Create Update Package		Windows 32...	SA108987	Highly Critical	23	07th June, 2...	31st May, 20...	4	60	0	0	64	28
Mozilla Fi...	Create Uninstall Package		Windows 64...	SA108987	Highly Critical	23	15th June, 2...	31st May, 20...	0	21	0	0	21	21
Google Cl...	Create Custom Package		Windows 32...	SA109412	Highly Critical	3	15th Septem...	22nd June, 2...	1	12	0	0	13	13
Google Cl...	Create Custom Package		Windows 64...	SA109412	Highly Critical	3	07th June, 2...	22nd June, 2...	1	4	0	0	5	5
IrfanView 4.x	4.60	IrfanView	Windows 32...	SA107469	Moderately	-	15th Septem...	18th March...	1	0	0	0	1	1
IrfanView 4.x	4.60	IrfanView	Windows 64...	SA107469	Moderately	-	03rd June, 2...	18th March...	1	0	0	0	1	1
Apple iTunes...	12.12.4	Apple	Windows 64...	SA108748	Highly Critical	23	24th April, 2...	18th May, 2...	2	0	0	0	2	2
Oracle Java...	11.0.15	Oracle Corpo...	Windows 64...	SA108171	Moderately	57	12th May, 2...	19th April, 2...	3	0	0	0	3	3
Oracle Java...	8u131	Oracle Corpo...	Windows 32...	SA108171	Moderately	57	12th May, 2...	19th April, 2...	4	0	0	0	4	4

48

## 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.

Home

Restart Service

Force Check-in

Save

Agent Deployment

Custom Package

Help

Feedback

About SVM Patch Publisher

Suitings

SVM Connection

Distribution Systems

Manage Patches

Flexera Package System (SPS)

Patch Template

Agent Deployment

Vendor Patch Module

Bring Your Own Patch (BYOP)

Flexera Package System (SPS)

Smart Groups: All Products

Configure View

Enter text to search...

Find

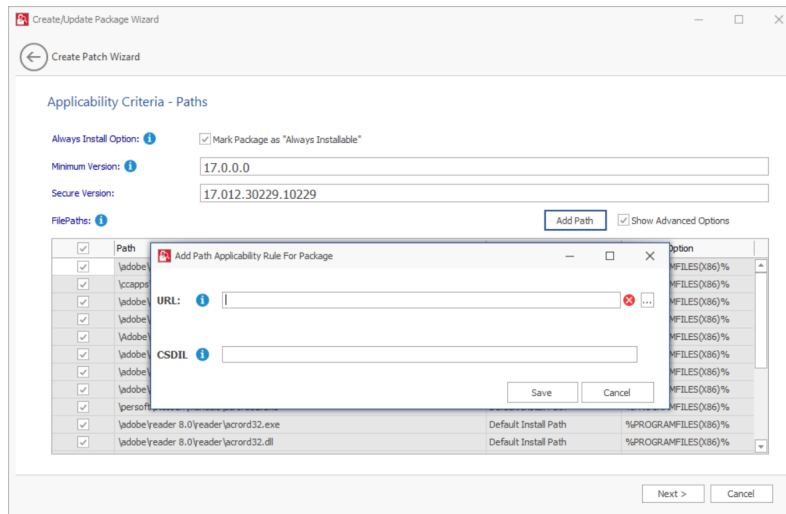
Product	Patched Versi...	Vendor	Architecture	SAID	Criticality	Threat Score	Detected	Advisory Publ...	Insecure	End-Of-Life	Secure	Total	Hosts	Uninstallable
UltraVNC 1.x	1.0.9.1		Windows 64...	SA41208	Moderately	-	10th March...	30th August...	2	0	0	0	2	1
Adobe Brack...	1.14.1	Adobe	Windows 32...	SA92461	Highly Critical	3	24th April, 2...	10th Decemb...	2	0	0	0	2	2
Adobe Acrob...	17.012.30229	Adobe	Windows 32...	SA107832	Highly Critical	2	15th June, 2...	12th April, 2...	1	0	0	0	1	1
Adobe Reader	22.x (Contin...	Adobe	Windows 32...	SA107832	Highly Critical	2	27th June, 2...	12th April, 2...	0	9	0	0	9	9
Amazon Corr...	8.332.08.1	Amazon.com	Windows 32...	SA107975	Moderately	6	15th Septem...	19th April, 2...	7	0	0	0	7	3
Amazon Corr...	Create Update Package		Windows 64...	SA107975	Moderately	6	23rd April, 2...	19th April, 2...	23	0	0	0	23	9
FileZilla	Create Uninstall Package		Windows 64...	SA94916	Moderately	-	03rd June, 2...	29th April, 2...	1	0	0	0	1	1
Mozilla	Create Custom Package		Windows 32...	SA108987	Highly Critical	23	07th June, 2...	31st May, 20...	4	60	0	0	64	28
Mozilla			Windows 64...	SA108987	Highly Critical	23	15th June, 2...	31st May, 20...	0	21	0	0	21	21
Google Chro...	103.x	Google	Windows 32...	SA109412	Highly Critical	3	15th Septem...	22nd June, 2...	1	12	0	0	13	13
Google Chro...	103.x	Google	Windows 64...	SA109412	Highly Critical	3	07th June, 2...	22nd June, 2...	1	4	0	0	5	5

## 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.

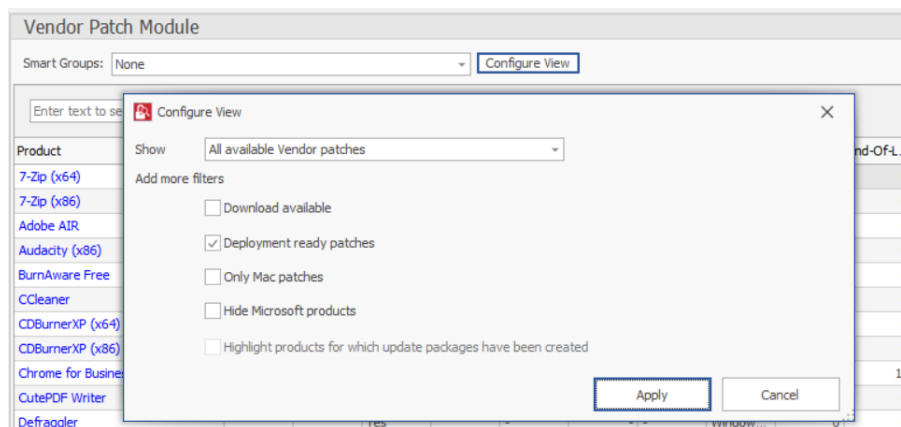
## Applicability Criteria - Paths Panel

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
<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 (Cloud Edition):

Issue	Description
<b>IOK-707192</b>	Changed API “action=get_host_scan_results” from “POST” to “GET”. For more information, see <a href="#">List Scan Result for Each Host</a> .
<b>IOK-706801</b>	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

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.