Software Vulnerability Manager (Cloud Edition) Release Notes

September 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:

- Software Vulnerability Manager and AdminStudio Integration
- Inventory - Based Vulnerability Assessment

- Support for Active Directory in SVM New User Interface
- Binary Versions

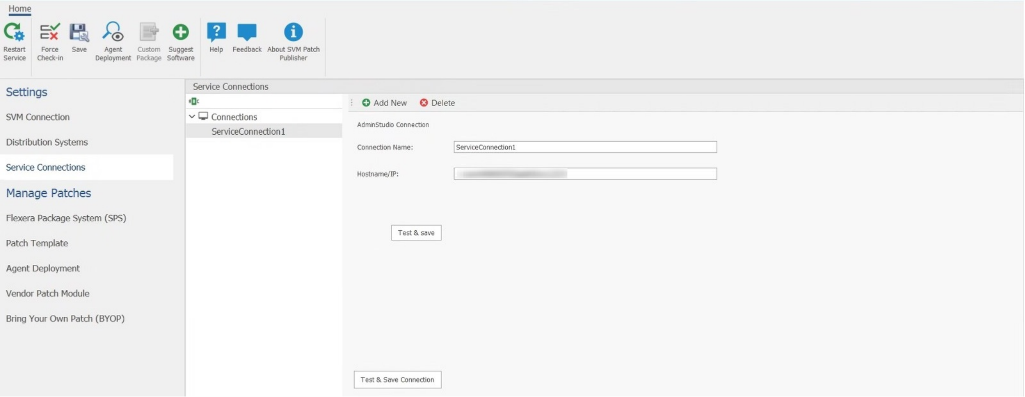
***Note** • To see the following new features and enhancements in your Software Vulnerability Manager (Cloud Edition) interface, you must refresh your browser's cache (press Ctrl+F5).*

Software Vulnerability Manager and AdminStudio Integration

AdminStudio is an industry de-facto tool for producing the best quality packages for deployment to endpoints.

In the Bring Your Own Patch (BYOP) view of SVM Patch Publisher, you will be able to send a request to AdminStudio for creating patches for the products which are not covered by SPS and VPM patches. Right click on a product for which you wish to send a request to AdminStudio for creating a patch and click on the menu option Request Patch.

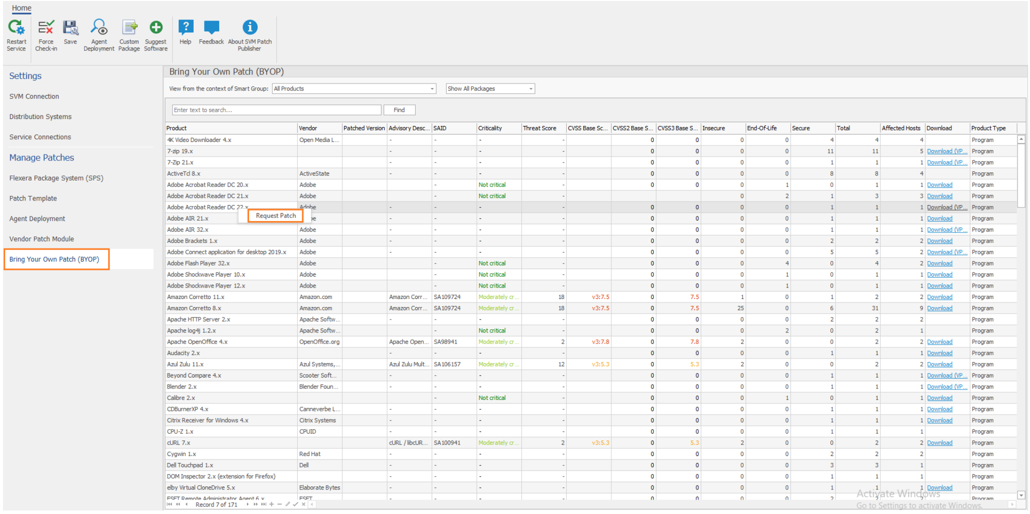
The new Service Connection view under the Settings menu provides options to establish connection between SVM and AdminStudio.



AdminStudio Connection

Connection Name: ServiceConnection1

Hostname/IP: [redacted]



View from the context of Smart Group: All Products

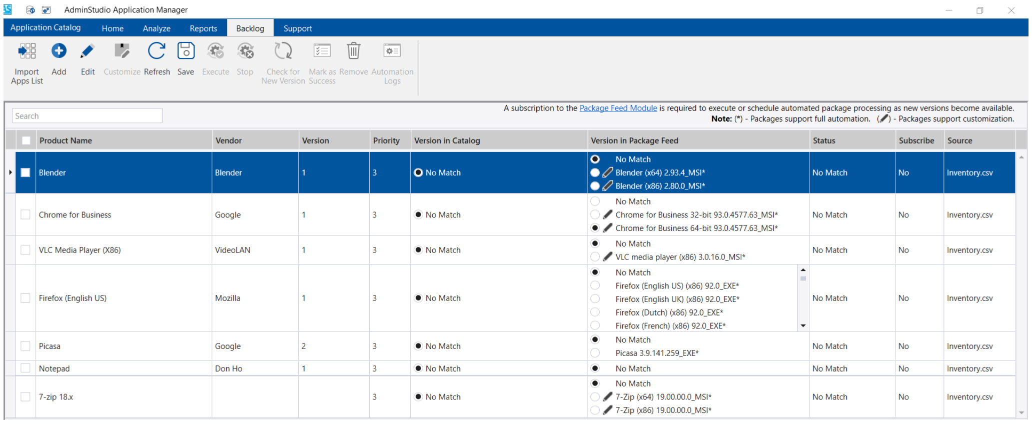
Show All Packages

Enter text to search...

Product	Vendor	Patched Version	Advisory Desc...	SAID	Criticality	Threat Score	CVSS Base Sc...	CVSS2 Base S...	CVSS3 Base S...	Insecure	End-Of-Life	Secure	Total	Affected Hosts	Download	Product Type
4K Video Downloader 4.x	Open Media L...		-	-	-	-		0	0	0	0	4	4	4		Program
7-zip 19.x			-	-	-	-		0	0	0	0	11	11	5	Download (VP...	Program
7-Zip 21.x			-	-	-	-		0	0	0	0	1	1	1	Download (VP...	Program
ActiveTcl 8.x	ActiveState		-	-	-	-		0	0	0	0	8	8	4		Program
Adobe Acrobat Reader DC 20.x	Adobe			-	Not critical	-		0	0	0	1	0	1	1	Download	Program
Adobe Acrobat Reader DC 21.x	Adobe			-	Not critical	-				0	2	1	3	3	Download	Program
Adobe Acrobat Reader DC 22.x	Adobe		-	-	-	-		0	0	0	0	1	1	1	Download (VP...	Program
Adobe AIR 21.x	be		-	-	-	-		0	0	0	0	1	1	1	Download	Program
Adobe AIR 32.x	Adobe		-	-	-	-		0	0	0	0	1	1	1	Download (VP...	Program
Adobe Brackets 1.x	Adobe		-	-	-	-		0	0	0	0	2	2	2	Download	Program
Adobe Connect application for desktop 2019.x	Adobe		-	-	-	-		0	0	0	0	5	5	2	Download (VP...	Program
Adobe Flash Player 32.x	Adobe			-	Not critical	-		0	0	0	4	0	4	2	Download	Program
Adobe Shockwave Player 10.x	Adobe			-	Not critical	-		0	0	0	1	0	1	1	Download	Program
Adobe Shockwave Player 12.x	Adobe			-	Not critical	-		0	0	0	1	0	1	1	Download	Program
Amazon Corretto 11.x	Amazon.com		Amazon Corr...	SA109724	Moderately cr...	18	v3:7.5	0	7.5	1	0	1	2	2	Download	Program
Amazon Corretto 8.x	Amazon.com		Amazon Corr...	SA109724	Moderately cr...	18	v3:7.5	0	7.5	25	0	6	31	9	Download	Program
Apache HTTP Server 2.x	Apache Softw...		-	-	-	-		0	0	0	0	2	2	2		Program
Apache log4j 1.2.x	Apache Softw...			-	Not critical	-		0	0	0	2	0	2	1		Program
Apache OpenOffice 4.x	OpenOffice.org		Apache Open...	SA98941	Moderately cr...	2	v3:7.8	0	7.8	2	0	0	2	2	Download	Program
Audacity 2.x			-	-	-	-		0	0	0	0	1	1	1	Download	Program
Azul Zulu 11.x	Azul Systems,...		Azul Zulu Mult...	SA106157	Moderately cr...	12	v3:5.3	0	5.3	2	0	0	2	2	Download	Program
Beyond Compare 4.x	Scooter Soft...		-	-	-	-		0	0	0	0	1	1	1	Download (VP...	Program
Blender 2.x	Blender Foun...		-	-	-	-		0	0	0	0	1	1	1	Download (VP...	Program
Calibre 2.x				-	Not critical	-		0	0	0	1	0	1	1	Download	Program
CDBurnerXP 4.x	Canneverbe L...		-	-	-	-		0	0	0	0	1	1	1	Download	Program
Citrix Receiver for Windows 4.x	Citrix Systems		-	-	-	-		0	0	0	0	1	1	1	Download	Program
CPU-Z 1.x	CPUID		-	-	-	-		0	0	0	0	1	1	1		Program
cURL 7.x			cURL / libcUR...	SA100941	Moderately cr...	2	v3:5.3	0	5.3	2	0	0	2	2	Download	Program
Cygwin 1.x	Red Hat		-	-	-	-		0	0	0	0	2	2	2		Program
Dell Touchpad 1.x	Dell		-	-	-	-		0	0	0	0	3	3	1		Program
DOM Inspector 2.x (extension for Firefox)			-	-	-	-		0	0	0	0	1	1	1		Program
elby Virtual CloneDrive 5.x	Elaborate Bytes		-	-	-	-		0	0	0	0	1	1	1	Download	Program
ESET Remote Administrator Agent 6.x	ESET		-	-	-	-		0	0	0	0	2	2	2		Program

Record 7 of 171

Patch requests sent to AdminStudio can be seen in the **Backlog** tab. The **Backlog** tab in AdminStudio helps you manage new and update software requests.



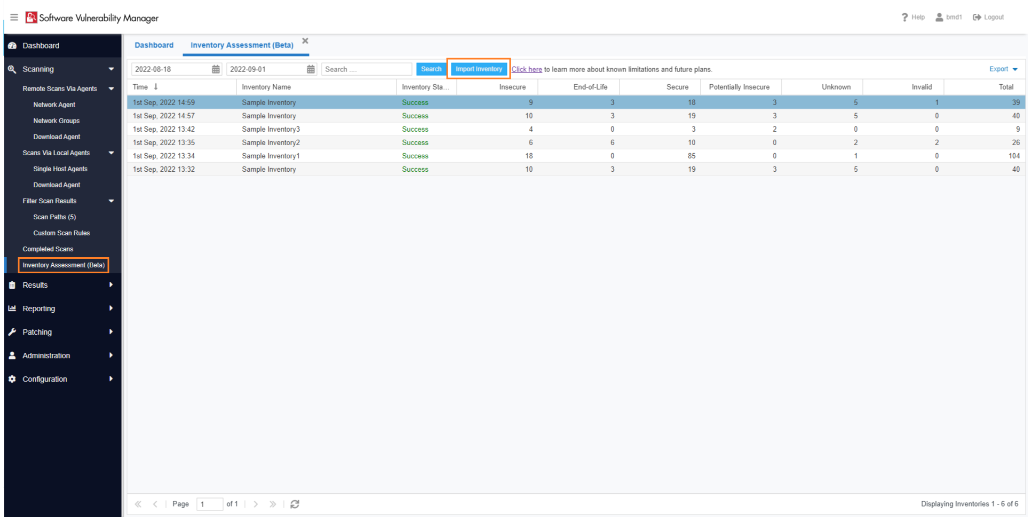
A subscription to the Package Feed Module is required to execute or schedule automated package processing as new versions become available.
Note: (*) - Packages support full automation. (✎) - Packages support customization.

□	Product Name	Vendor	Version	Priority	Version in Catalog	Version in Package Feed	Status	Subscribe	Source
□	Blender	Blender	1	3	● No Match	● No Match ○ ✎ Blender (x64) 2.93.4_MSI* ○ ✎ Blender (x86) 2.80.0_MSI*	No Match	No	Inventory.csv
□	Chrome for Business	Google	1	3	● No Match	○ No Match ○ ✎ Chrome for Business 32-bit 93.0.4577.63_MSI* ● ✎ Chrome for Business 64-bit 93.0.4577.63_MSI*	No Match	No	Inventory.csv
□	VLC Media Player (X86)	VideoLAN	1	3	● No Match	● No Match ○ ✎ VLC media player (x86) 3.0.16.0_MSI*	No Match	No	Inventory.csv
□	Firefox (English US)	Mozilla	1	3	● No Match	● No Match ○ Firefox (English US) (x86) 92.0_EXE* ○ Firefox (English UK) (x86) 92.0_EXE* ○ Firefox (Dutch) (x86) 92.0_EXE* ○ Firefox (French) (x86) 92.0_EXE*	No Match	No	Inventory.csv
□	Picasa	Google	2	3	● No Match	● No Match ○ Picasa 3.9.141.259_EXE*	No Match	No	Inventory.csv
□	Notepad	Don Ho	1	3	● No Match	● No Match	No Match	No	Inventory.csv
□	7-zip 18.x			3	● No Match	● No Match ○ ✎ 7-Zip (x64) 19.00.00.0_MSI* ○ ✎ 7-Zip (x86) 19.00.00.0_MSI*	No Match	No	Inventory.csv

Inventory - Based Vulnerability Assessment

A new menu item - **Inventory Assessment** is added under **Scanning** menu. The file containing the software inventory is expected to be in the .csv format. To import an inventory in SVM for vulnerability assessment, click **Import Inventory** button.

This beta feature provides directional (less definitive than file-level scan using file signatures) inventory assessment results depending largely upon the detail of the version information contained in the supplied inventory data.



Click here to learn more about known limitations and future plans.

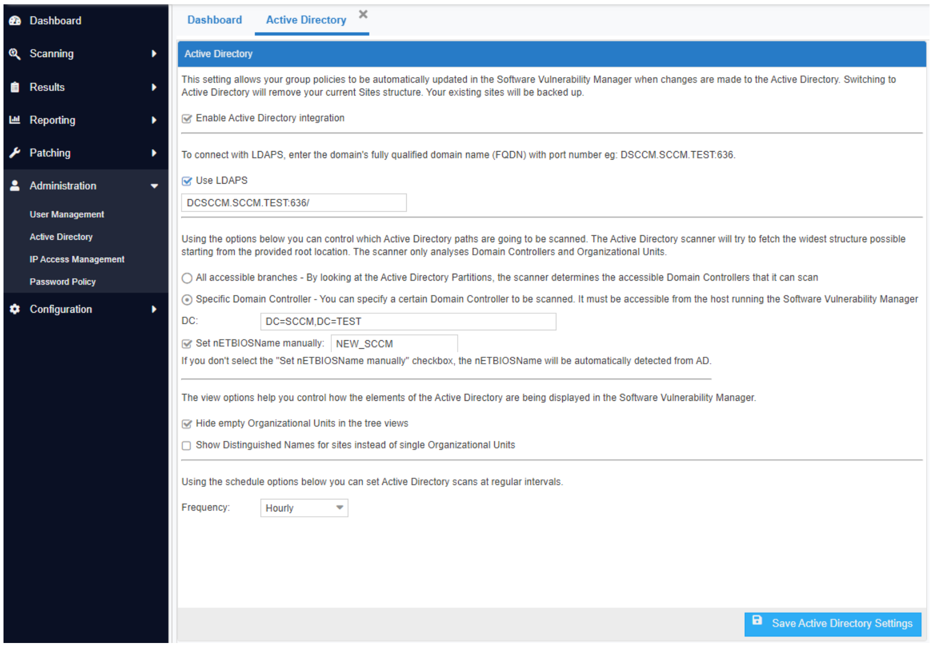
Time	Inventory Name	Inventory Sta...	Insecure	End-of-Life	Secure	Potentially Insecure	Unknown	Invalid	Total
1st Sep, 2022 14:59	Sample Inventory	Success	9	3	18	3	5	1	39
1st Sep, 2022 14:57	Sample Inventory	Success	10	3	19	3	5	0	40
1st Sep, 2022 13:42	Sample Inventory3	Success	4	0	3	2	0	0	9
1st Sep, 2022 13:35	Sample Inventory2	Success	6	6	10	0	2	2	26
1st Sep, 2022 13:34	Sample Inventory1	Success	18	0	85	0	1	0	104
1st Sep, 2022 13:32	Sample Inventory	Success	10	3	19	3	5	0	40

Page 1 of 1

Displaying Inventories 1 - 6 of 6

Support for Active Directory in SVM New User Interface

With this update, you can now configure Active Directory scan and use the schedule options to set Active Directory scans at selected intervals using daemon.



This setting allows your group policies to be automatically updated in the Software Vulnerability Manager when changes are made to the Active Directory. Switching to Active Directory will remove your current Sites structure. Your existing sites will be backed up.

☑ Enable Active Directory integration

To connect with LDAPS, enter the domain's fully qualified domain name (FQDN) with port number eg: DSCCM.SCCM.TEST:636.

☑ Use LDAPS

DCSCCM.SCCM.TEST:636/

Using the options below you can control which Active Directory paths are going to be scanned. The Active Directory scanner will try to fetch the widest structure possible starting from the provided root location. The scanner only analyses Domain Controllers and Organizational Units.

○ All accessible branches - By looking at the Active Directory Partitions, the scanner determines the accessible Domain Controllers that it can scan

● Specific Domain Controller - You can specify a certain Domain Controller to be scanned. It must be accessible from the host running the Software Vulnerability Manager

DC: DC=SCCM,DC=TEST

☑ Set nETBIOSName manually: NEW_SCCM

If you don't select the "Set nETBIOSName manually" checkbox, the nETBIOSName will be automatically detected from AD.

The view options help you control how the elements of the Active Directory are being displayed in the Software Vulnerability Manager.

☑ Hide empty Organizational Units in the tree views

□ Show Distinguished Names for sites instead of single Organizational Units

Using the schedule options below you can set Active Directory scans at regular intervals.

Frequency: Hourly

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 v7.3.790 (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.

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-927687	Patch Publisher showing wrong download URL for SVM agent.

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

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.