

Software Vulnerability Manager (Cloud Edition) Release Notes

August 2023

Introduction	1
New Features and Enhancements	1
Software Vulnerability Manager User Interface Enhancements	2
Configure Scan Exclusion Paths	2
Add to Block List from Installations Window	4
Split CSV Report into Smaller Multiple Files	4
Reference: Latest Binary Versions	5
Resolved Issues	5
Community Blogs	5
Product Feedback	5
Legal Information	6

Introduction

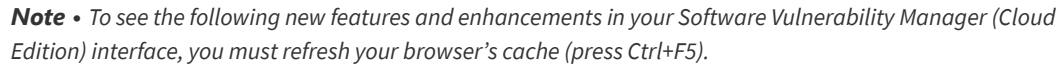
Flexera's Software Vulnerability Manager is a software vulnerability and patch management solution that facilitates a customized patch management process. It combines vulnerability and threat intelligence, end point assessment, and patch creation and publishing enable an informed and rapid patch management.

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:

- [Software Vulnerability Manager User Interface Enhancements](#)
- [Reference: Latest Binary Versions](#)



The following improvements have been added to the Software Vulnerability Manager User Interface.

- ## Configure Scan Exclusion Paths

Software Vulnerability Manager

Dashboard Settings Log Messages

General Windows Update Single Sign-On Email/SMS Recipients

Stop Site update

Java Assessment Settings

I want to detect all instances of Java, including those included with other applications which cannot be remediated by a Java patch. By default, only standard installation directories are considered as only they can be directly patched. To patch vulnerable versions of Java embedded in other applications, such applications need to be patched versus trying to update Java directly. If enabling detection anywhere Java is found, look to the detected paths to determine which can or cannot be patched directly.

☒ Detect Java only in standard installation directories where it can be patched

☐ Detect Java only in any directories where it is found, including those that cannot be directly patched

Scan Exclusion Paths

Below are the list of file paths or folders match added by default to exclude from scan result. Desired approach is to select all items in the list below:

<input type="checkbox"/>	File path match	Regex
<input checked="" type="checkbox"/>	C:\ cache (upper case)	SYSTEM\VOLCACHE
<input checked="" type="checkbox"/>	c:\OSTORE	DWSTORE
<input checked="" type="checkbox"/>	C:\ cache (lower case)	system32\cache
<input type="checkbox"/>	Installer	Installer
<input checked="" type="checkbox"/>	%ServicePackUninstall%	%ServicePackUninstall%
<input checked="" type="checkbox"/>	Patch Cache	PatchCache\$
<input checked="" type="checkbox"/>	RECYCLER	RECYCLER
<input checked="" type="checkbox"/>	Recycle Bin	\$Recycle Bin
<input checked="" type="checkbox"/>	Registered Packages	RegisteredPackages
<input checked="" type="checkbox"/>	ServicePackFiles	ServicePackFiles
<input checked="" type="checkbox"/>	SoftwareDistribution	SoftwareDistribution
<input checked="" type="checkbox"/>	System Volume Information	SystemVolumeInformation
<input checked="" type="checkbox"/>	Temp	\WINNT\Temp
<input checked="" type="checkbox"/>	Uninstall Path	\$Uninstall
<input checked="" type="checkbox"/>	WinSxS	WinSxS
<input checked="" type="checkbox"/>	_H_mig	_H_mig\$
<input checked="" type="checkbox"/>	ieUpdates	ieUpdates
<input checked="" type="checkbox"/>	ntservicepackuninstall	ntservicepackuninstall\$
<input checked="" type="checkbox"/>	winsxs x86	winsxs\x86

Save

Software Vulnerability Manager (Cloud Edition) (August 2023)

Software Vulnerability Manager

Dashboard
Scanning
Results
Reporting
Patching
Administration
Configuration
Settings
Log Messages
Activity Log
Software Suggestions
Security
Change Password
Password Recovery


Dashboard

Activity Log

Show all logs
From: 2023-05-11
To: 2023-06-11
Search type: Exclusion Path List
Search text:
Search
Show Priorities
Create


Activity Name	Activity Status	U...	Time	Activity Information	Host	Priority
Exclusion Path List	Successful	p7...	1...	List of Excluded Paths: Temp, Recycle Bin	159.117.152.221	Low
Exclusion Path List	Successful	p7...	1...	List of Excluded Paths: winssxs x86, i.e/updates, hf_mig, System Volume Information	159.117.152.221	Low
Exclusion Path List	Successful	p7...	0...	List of Excluded Paths: winssxs x86, i.e/updates, hf_mig, System Volume Information	159.117.152.221	Low
Exclusion Path List	Successful	p7...	1...	List of Excluded Paths: winssxs x86, i.e/updates, hf_mig, System Volume Information	159.117.152.221	Low
Exclusion Path List	Successful	p7...	1...	List of Excluded Paths: Installer	159.117.152.221	Low
Exclusion Path List	Successful	p7...	1...	List of Excluded Paths: Temp, Recycle Bin	159.117.152.221	Low
Exclusion Path List	Successful	p7...	1...	List of Excluded Paths: Temp, Recycle Bin	159.117.152.221	Low
Exclusion Path List	Successful	p7...	1...	List of Excluded Paths: Temp, Recycle Bin	159.117.152.221	Low
Exclusion Path List	Successful	p7...	1...	List of Excluded Paths: Temp, Recycle Bin	159.117.152.221	Low
Exclusion Path List	Successful	p7...	1...	List of Excluded Paths: Temp, Recycle Bin	159.117.152.221	Low
Exclusion Path List	Successful	p7...	1...	List of Excluded Paths: Temp, Installer	159.117.152.221	Low
Exclusion Path List	Successful	p7...	1...	List of Excluded Paths: Temp, Installer	159.117.152.221	Low
Exclusion Path List	Successful	p7...	1...	List of Excluded Paths: i.e/updates, hf_mig, Uninstall Path, Temp, RegisteredPacka...	159.117.152.221	Low
Exclusion Path List	Successful	p7...	1...	List of Excluded Paths: Installer	159.117.152.221	Low
Exclusion Path List	Successful	p7...	1...	List of Excluded Paths: hf_mig, Temp, Recycle Bin	159.117.152.221	Low
Exclusion Path List	Successful	p7...	1...	List of Excluded Paths: Recycle Bin, Temp	159.117.152.221	Low


In the old SVM user interface, excluded paths will be displayed in the **Configuration > Settings > Scan Exclusion Paths**.




Software Vulnerability Manager


Menu


 Dashboard


 Scanning


- Remote Scanning Via Agents
 - Network Appliance Agents
 - Network Appliance Groups
 - Download Network Agent
- Scanning Via Local Agents
 - Single Host Agents
 - Download Local Agent
- Filter Scan Results
 - Scan Paths (1)
 - Custom Scan Rules
 - Completed Scans

 Results


 Reporting

 Patching

 Administration

 Configuration

- Settings
- Log Messages
- Activity Log

 Security

- Change Password
- Password Recovery Settings

Software Vulnerability Manager Settings

Windows Update Settings

Configure the behaviour of the Windows Update Agent (WUA). (?)

☐ Use a managed Windows Update server

☐ Use the official Windows Update server

☐ Use the official Microsoft Update server

☐ Use offline method: path to .CAB file

☐ Enable WMI Check

Clear

Save Windows Updates Settings

Windows Update Proxy Settings

Configure whether the Windows Update Agent uses a proxy server.

☒ Do not use a proxy server for the Windows Update Agent

☐ Use the same proxy server for the Windows Update Agent as the Software Vulnerability Manager Agent uses

☐ Use a custom proxy server for the Windows Update Agent

Save Windows Update Agent Proxy Settings

IdP Configuration Instructions

Single Sign On URL (Same with Recipient URL and Destination URL) (?)

Account Key

Set the below value in your Identity Provider (IdP) as a SAML attribute named "accountKey"

Generate Key

Note: This key is not stored on the Software Vulnerability Manager server, please make sure that you keep it in a safe place. If lost, you may regenerate the key but doing so will invalidate the old key.

Service Provider Metadata URL

Service Provider Configuration

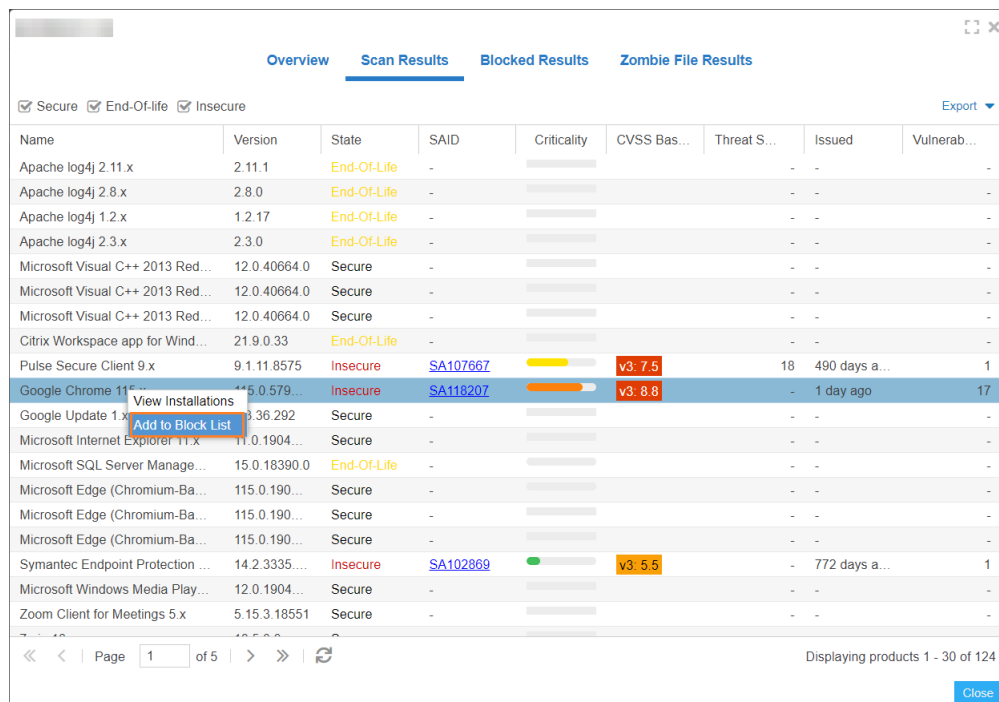
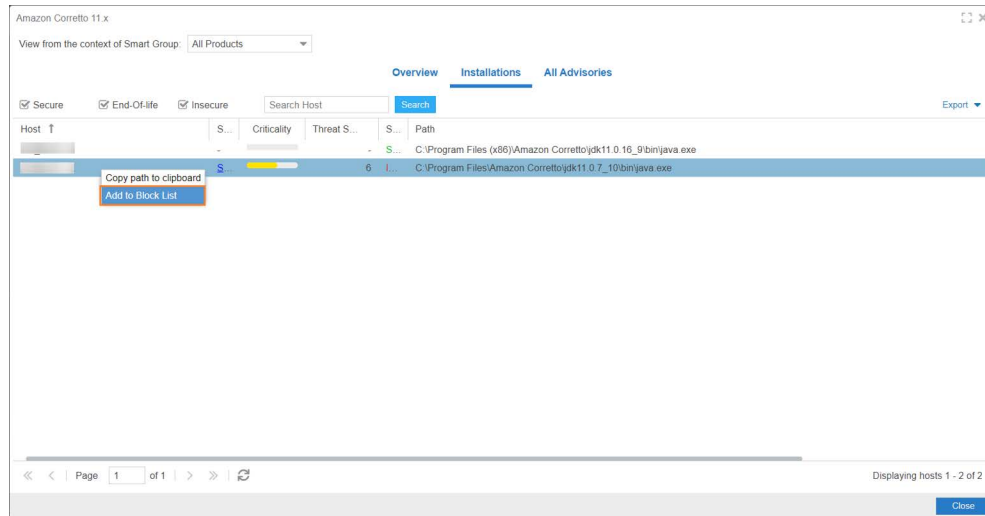
Scan Exclusion Paths

Excluded Paths: [Installer \(?\)](#)

Add to Block List from Installations Window

A new **Add to Block List** option is added in the context menu under the Smart Groups / Completed Scans > Installations window. By selecting this option, the selected host / product will be added to the Block List.

To do so, right click on selected row and choose **Add to Block List** from the context menu.



Split CSV Report into Smaller Multiple Files

While generating reports that may result in large-sized CSV files, the file will be split into multiple smaller of approximately 500 MB each. This enhancement will improve performance and eliminate the possibility of report failure.

Reference: Latest 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 v7.13.1053 (to download, [click here](#)) (no change)
- 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.

Resolved Issues

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

Issue	Description
IOK-1058944	SVM daemon scheduled export not working.

Community Blogs

Please subscribe to latest posts about Software Vulnerability Manager by going to <https://community.flexera.com/t5/Software-Vulnerability/bg-p/SoftwareVulnerabilityManagementblog> and clicking on subscribe.

Please subscribe to latest release announcements concerning Software Vulnerability Manager by going to <https://community.flexera.com/t5/Software-Vulnerability/bg-p/Software-Vulnerability-Release-blog> 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.