

Software Vulnerability Manager (On-Premises Edition) Release Notes

September 2023

Introduction	1
New Features and Enhancements	2
Patch Publisher Enhancements	2
Devices View	2
Custom Scan Rules View	3
View Scan Result for Hosts/Devices	3
Highlight the Published Products in the Flexera Package System (SPS) View	4
Software Vulnerability Manager User Interface Enhancements	4
Display Zombie Files	5
Configure Scan Exclusion Paths	5
Flexera System Score Enhancements	7
Add to Block List from Installations Window	8
Highlight the Published Products in the Flexera Package System (SPS) View	9
Split CSV Report into Smaller Multiple Files	10
Reference: Latest Binary Versions	10
Known Issues	10
Resolved Issues	11
Community Blogs	11
Product Feedback	11
Legal Information	11

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 via Microsoft® Intune, VMware® Workspace One, or BigFix.

SVM Patch Publisher inherits its current functionalities from the Patch Daemon. SVM Patch Publisher enables you to configure connections to the SVM server and to the supported end point management systems. The tool polls SVM on a configured frequency to look for new patches resulting either from a manual publish or Patch Automation to publish patches to the specified end point management system.

New Features and Enhancements

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

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



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).

Patch Publisher Enhancements

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

- [Devices View](#)
- [Custom Scan Rules View](#)
- [View Scan Result for Hosts/Devices](#)
- [Highlight the Published Products in the Flexera Package System \(SPS\) View](#)

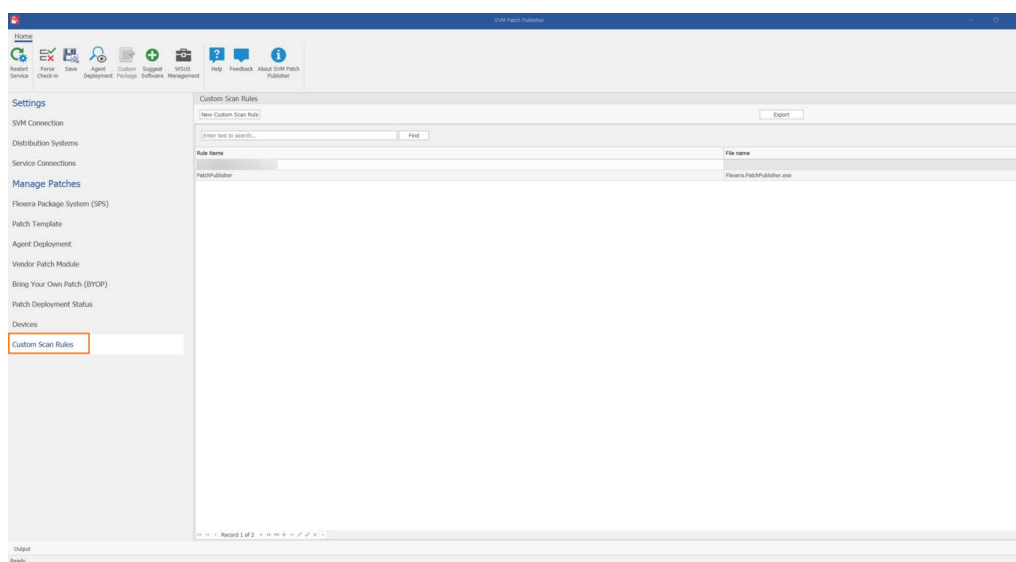
Devices View

A new **Devices** view is introduced under the **Manage Patches** menu. The **Devices** view displays the hosts/devices based on the Host Smart Group that is selected from the **Smart Group** drop-down.

Device	System Score	Last Scan	Insecure	End-Of-Life	Secure	Total	Site Name	Scan Engine	Software Platform
273 FLORIDA	96	31st Aug. 2023	114	34	125	273	FLORIDA	7.6.0.24	Windows
79 SIMPSON	94	31st Aug. 2023	9	4	66	79	SIMPSON	7.6.0.22	Windows
80 WORKGROUP	93	27th Aug. 2023	9	1	80	80	WORKGROUP	7.6.0.24	Windows
26 Active Directory: orphans.20	94	22nd Jun. 2023	2	0	34	26	Active Directory: orphans.20	7.6.0.24	Windows
20 Active Directory: orphans.20	96	22nd Jun. 2023	0	1	25	20	Active Directory: orphans.20	Confly Manager	Confly Manager
27 Active Directory: orphans.20	91	24th Jul. 2023	4	2	46	27	Active Directory: orphans.20	7.6.0.24	Windows
414 Active Directory: orphans.20	93	12th Aug. 2023	30	34	350	414	Active Directory: orphans.20	7.6.0.24	Windows
68 WORKGROUP	68	31st Aug. 2023	1	21	46	68	WORKGROUP	7.6.0.24	Windows
287 Rhinelle	100	20th Aug. 2023	0	0	287	287	Rhinelle	Red Hat Linux	Red Hat Linux
82 SHIPRAI	99	20th Aug. 2023	11	2	67	82	SHIPRAI	7.6.0.24	Windows
114 Rhinelle	74	30th Aug. 2023	30	0	84	114	Rhinelle	Red Hat Linux	Red Hat Linux

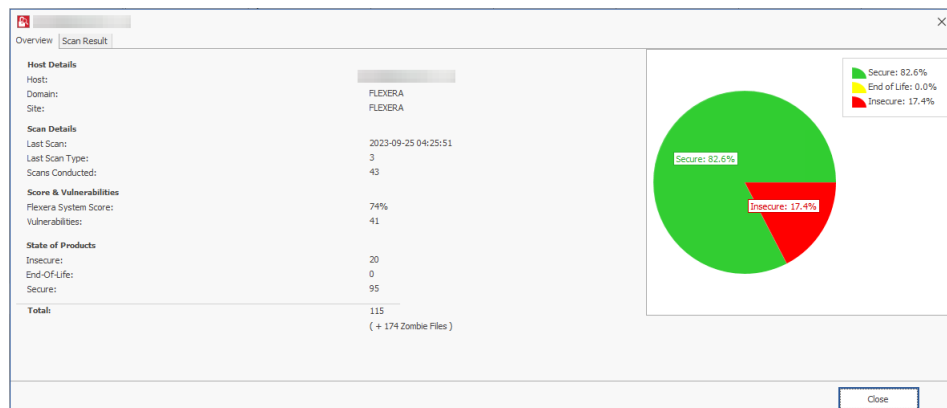
Custom Scan Rules View

A new **Custom Scan Rules** view is introduced under the **Manage Patches** menu. Use the **Custom Scan Rules** page to create and maintain custom rules for scanning customer created programs, drivers, and plug-ins.



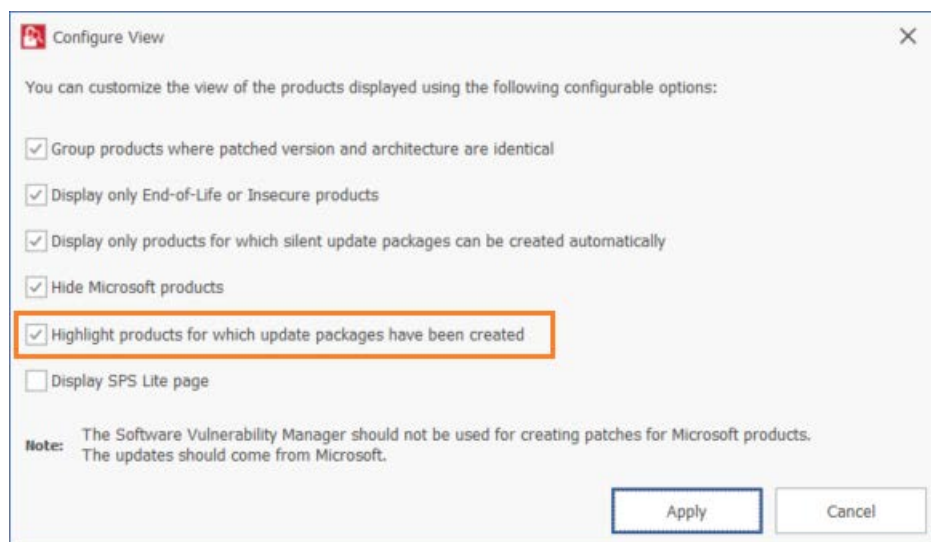
View Scan Result for Hosts/Devices

In the **Devices** view, you can view scan result for the hosts/devices based on the Host Smart Group that is selected from the **Smart Groups** drop-down. To do so, right click on selected device and choose **View Scan Result** from the context menu. A popup appear with details of the scan result for the selected host/device.



Highlight the Published Products in the Flexera Package System (SPS) View

In the **Flexera Package System (SPS) > Configuration View** dialog box, the **Highlight product for which update packages have been created** option is now enabled to check/uncheck to highlight the products for which an update package is created and published to a configured endpoint management system.



Software Vulnerability Manager User Interface Enhancements

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

- [Display Zombie Files](#)
- [Configure Scan Exclusion Paths](#)
- [Flexera System Score Enhancements](#)
- [Add to Block List from Installations Window](#)

- Highlight the Published Products in the Flexera Package System (SPS) View
- Split CSV Report into Smaller Multiple Files

Display Zombie Files

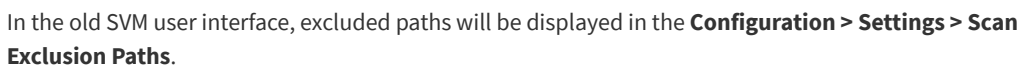
A new **Display Zombie Files** check box is introduced in the **Configuration view > Settings > General > Zombie File Settings**. The **Display Zombie Files** check box option enables only when the **Hide Zombie Files** option is unchecked. By selecting the **Display Zombie Files** option and running the scan, the discovered zombie files will be displayed in the **Scanning > Completed Scans > View Scan Result > Zombie File Results** tab.

The screenshot shows the 'Software Vulnerability Manager' interface. In the 'Configuration' view, the 'Settings' tab is active, and the 'Zombie File Settings' section is expanded. The 'Display Zombie Files' checkbox is checked and highlighted with a red box. Below the settings, the 'Zombie File Results' tab is selected, displaying a table of discovered zombie files.

Name	Version	State	SAID	Path	Criticality	CVSS Base Score	Threat	Issued	Vulnerability
Microsoft Visual C++ 20...	11.0.5072...	Secure	-	C:\Windows\SysWOW64\msvc110.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.29.301...	Secure	-	C:\Program Files (x86)\AdminStudio2022\Repackager\msvc140.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.0.2421...	Secure	-	C:\Program Files (x86)\Microsoft Intune Management Extension\msvc140.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.34.319...	Secure	-	C:\Program Files (x86)\Microsoft Edge\Application\115.0.1901.188\msvc140.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.34.319...	Secure	-	C:\Program Files (x86)\Microsoft EdgeCore\115.0.1901.188\msvc140.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.34.319...	Secure	-	C:\Program Files (x86)\Microsoft EdgeWebView\Application\115.0.1901.188\msvc140.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.16.270...	Secure	-	C:\Program Files (x86)\Mozilla Thunderbird\msvc140.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.28.293...	Secure	-	C:\Program Files (x86)\Zoom\bin\msvc140.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.28.293...	Secure	-	C:\Program Files (x86)\Zoom\bin\msvc140.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.16.270...	Secure	-	C:\Program Files\Mozilla Firefox\msvc140.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.16.270...	Secure	-	C:\Program Files\Mozilla Thunderbird\msvc140.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.16.270...	Secure	-	C:\Program Files\WindowsApps\Microsoft.Microsof3DViewer_7.2211.24012.0_x64_8weky03d8bwe140.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.29.301...	Secure	-	C:\Program Files\WindowsApps\Microsoft.SkypeApp_15.96.3207.0_x64_8weky03d8bwe140.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.29.301...	Secure	-	C:\Program Files\WindowsApps\Microsoft.SkypeApp_15.96.3207.0_x64_8weky03d8bwe140.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.30.307...	Secure	-	C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00.UWPDesktop_14.0.30704.0_x64_8weky03d8bwe140.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.30.307...	Secure	-	C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00.UWPDesktop_14.0.30704.0_x64_8weky03d8bwe140.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.32.313...	Secure	-	%USERPROFILE%\AppData\Local\Microsoft\OneDrive\23.061.0319.0003\msvc140.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.24.281...	Secure	-	C:\Windows\System32\msvc140.dll	Low	0.0	-	-	-
Microsoft Visual C++ 20...	14.31.311...	Secure	-	C:\Windows\SysWOW64\msvc140.dll	Low	0.0	-	-	-
Microsoft Windows Defe...	4.18.1909.6	Secure	-	C:\Program Files\Windows Defender\MpEng.exe	Low	0.0	-	-	-
Microsoft Windows Defe...	4.18.2305...	Secure	-	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.23050.5-0\MpEng.exe	Low	0.0	-	-	-
Microsoft XML Core Ser...	6.30.1439...	Secure	-	C:\Program Files (x86)\AdminStudio2022\QualityMonitor\msxm6.dll	Low	0.0	-	-	-

Configure Scan Exclusion Paths

A new **Scan Exclusion Paths** is introduced under the **Configuration view > Settings**. By default, all paths will be selected and these paths are not included in scan result. Uncheck desired path to include in the scan result.



Software Vulnerability Manager Settings

Windows Update Settings

Configure the behaviour of the Windows Update Agent (WUA). (2)

☐ 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) (2)

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 (2)

Flexera System Score Enhancements

You can now configure the calculation of the Flexera System Score. A new **System Score Settings** is introduced under the **Configuration** view > **Settings**. In the **System Score Settings**, you can configure weightage for each criterion to calculate the system score for hosts. The sum of all weights cannot exceed 100.

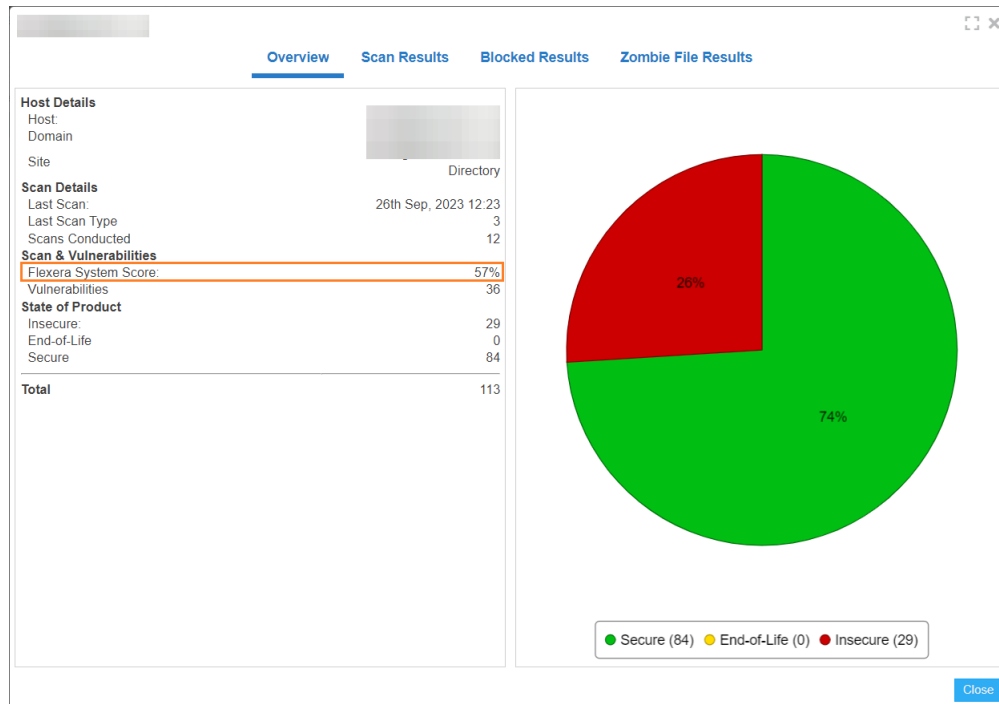
System Score Settings

The System Score for a host is calculated based on the following attributes. The percentage assigned to each attribute will dictate its influence on the overall calculation of the system score. The sum of all weights cannot exceed 100. (2)

Secure Products	60	%
Zero Day	10	%
Threat Score	10	%
CVSS Score	10	%
Criticality	10	%

Save

Upon defining the criteria and running the scan, the system score details will be displayed in the **Scanning** > **Completed Scans** > **View Scan Result** > **Overview** tab. Also displayed in the **Host Smart Groups** grid.



Software Vulnerability Manager

Dashboard Host: All Hosts

Showing All Sites Showing All Platforms Search Last Compiled: 27th Sep, 2023 13:00 Export

Host	System Score	Last Scan	Insecure	End-Of-Life	Secure	Total	Site Name	Scan Engine	Software Platform
	62%	24th Sep, 2023 ...	12	26	93	131	Active Directory ...	7.6.0.24	Windows
	100%	17th Aug, 2023 ...	0	0	2	2	FLEXERA	7.6.0.24	Windows
	99%	25th Sep, 2023 ...	9	0	79	88	Active Directory ...	7.6.0.24	Windows
	53%	25th Sep, 2023 ...	5	0	206	211	Active Directory ...	RHEL 7.6.0.24	Red Hat Linux

In the old SVM user interface, configured criteria details will be displayed in the **Configuration > Settings > System Score Settings**. These attributes are not editable.

System Score Settings

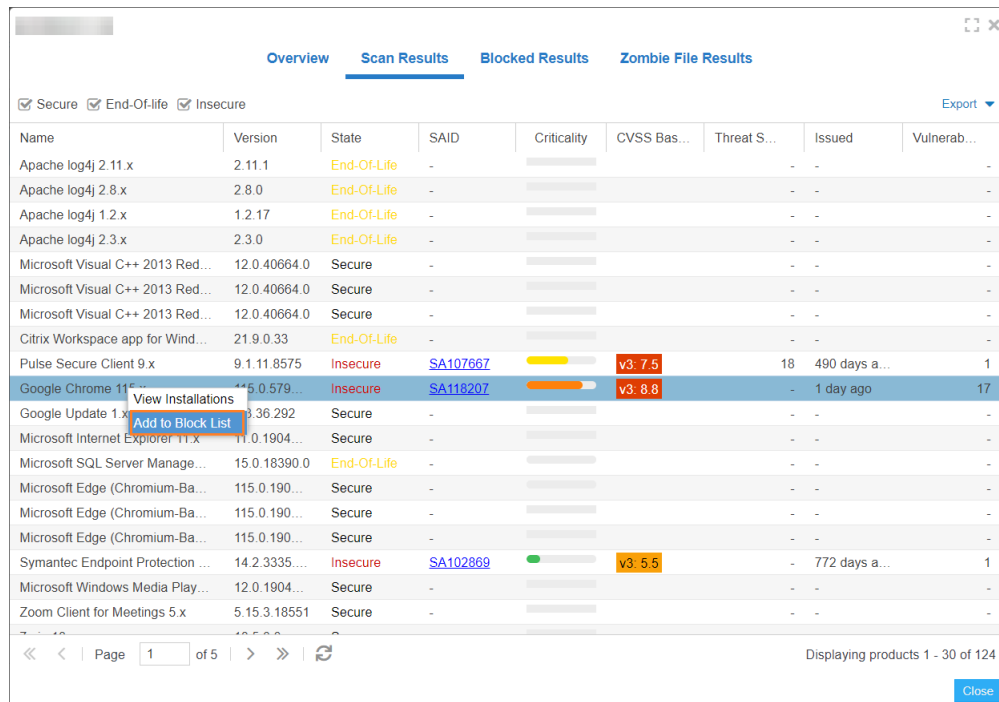
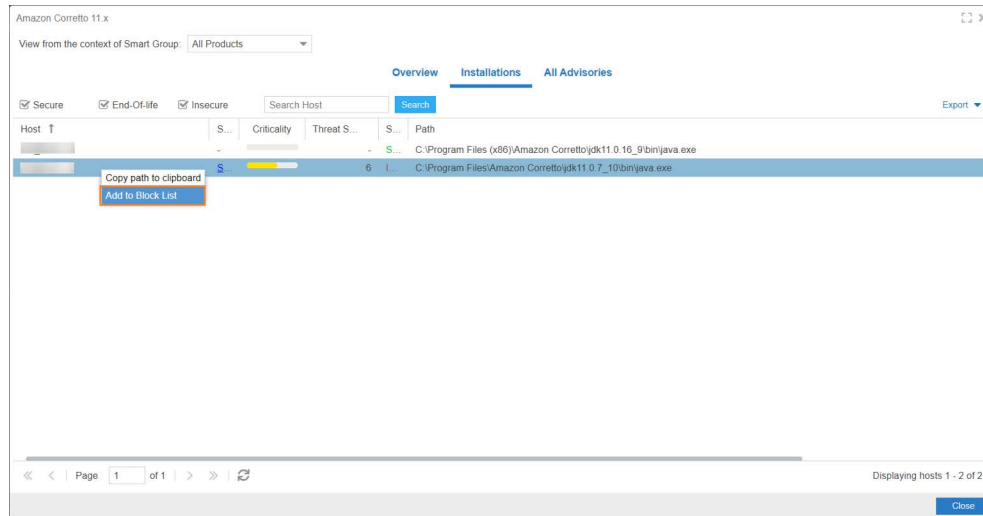
The System Score for a host is calculated based on the following attributes. The percentage assigned to each attribute will dictate its influence on the overall calculation of the system score. The sum of all weights cannot exceed 100. (?)

- Secure Products: 60%
- Zero day: 10%
- Threat Score: 10%
- CVSS Score: 10%
- Criticality: 10%

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.



Highlight the Published Products in the Flexera Package System (SPS) View

In the **Flexera Package System (SPS) > Configuration View** dialog box, the **Highlight product for which update packages have been created** option is now enabled to check/uncheck to highlight the products for which update package is created and published to a configured endpoint management system.

Configure View

You can customize the view of the products displayed using the following configurable options:

☒ Group products where patched version and architecture are identical

☒ Display only End-of-Life or Insecure products

☒ Display only products for which silent update packages can be created automatically

☒ Hide Microsoft products

☒ Highlight products for which update packages have been created

☐ Display SPS Lite page

Note: The Software Vulnerability Manager should not be used for creating patches for Microsoft products. The updates should come from Microsoft.

Apply

Cancel

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 v7.6.1.24 (no change)
- Single Host Agent v7.6.1.24 (no change)
- SVM Daemon v7.6.1.24 (no change)
- SVM System Center Plugin v7.6.1.24 (no change)
- SVM Patch Publisher v7.15.1071 (to download, [click here](#))

Refer “Patch Publisher Enhancements” for changelog.

- SVM On-Prem Client Toolkit v5.0.547 (to download, [click here](#)) (no change)

Known Issues

The following table lists the known issues in Software Vulnerability Manager (On-Premises Edition):

Issue	Description
IOK-1046547	WSUS Management tool is giving exception when it is relaunched.

Resolved Issues

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

Issue	Description
IOK-1047459	Unable to download CSV report.
IOK-1042693	Unable to download non-enhanced packages.
IOK-752509	Unable to save SSO settings in SVM old console.
IOK-1055008	On Creating/Editing the Patch Template, updated message in the output window saying template created/updated successfully.
IOK-1040911	In the Report Configuration grid, unable to download the reports when Download column is moved.
IOK-1057377	While suggesting a software from the Patch Publisher, Version is not coming properly.
IOK-1059191	In the Patch Publisher > Patch Deployment Status grid, on deleting any failed package an exception popup appears.
IOK-1065430	In the Patch Publisher, when you publish a custom package from the Custom package in the ribbon, giving an error message.

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.