flexera...

Software Vulnerability Manager (Cloud Edition) Release Notes

July 2023

| Introduction | 1 |
|--|---|
| New Features and Enhancements | 1 |
| | |
| Patch Publisher Enhancements | |
| Custom Scan Rules View | |
| Software Vulnerability Manager User Interface Enhancements | 2 |
| Display Zombie Files | 2 |
| Reference: Latest Binary Versions | 3 |
| Resolved Issues | 4 |
| Community Blogs | 4 |
| Community Blogs | |
| Product Feedback | 4 |
| | - |
| Legal Information | 5 |

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 (thirdparty) 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:

- 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 (Cloud Edition) interface, you must refresh your browser's cache (press Ctrl+F5).

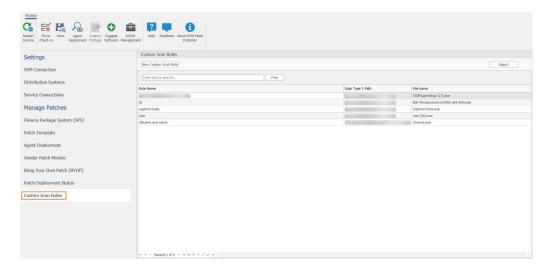
Patch Publisher Enhancements

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

Custom Scan Rules View

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.



Software Vulnerability Manager User Interface Enhancements

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

Display Zombie 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.

? Help 🚨 🗰 🕪 Logout

| 😑 🖪 Software Vulneral | bility Manager ? Help 🛔 👘 Laport | | | | | |
|---|---|--|--|--|--|--|
| Dashboard | Dashboard Settings × | | | | | |
| Q Scanning | General Windows Update Single Sign-On Email/SMS Recipients | | | | | |
| Results | - Line Update | | | | | |
| 🗠 Reporting | results not being the most accurate representation of the current state of my network. (2) @ Activate Live Lipote | | | | | |
| | Collect Network Information | | | | | |
| Administration | I want to allow the collection and storage of network information, such as assigned IPs and MAC addresses, when I scan devices. (2) (2) Allow Collection of Network Information | | | | | |
| Configuration Settings Log Messages Activity Log | - 2010/bit File Setting: This setting determines the behaviour of the scan engine for handling zonable files. If you choose to hide the zonable files, they will not be included in any of the scan results. If you choose to display zonable files, they will be displayed under the Zonable File Setting to the scan results. If you choose to display zonable files, they will be displayed under the Zonable File Setting to the scan results. If you choose to display zonable files, they will be displayed under the Zonable File Setting to the scan results. If you choose to display zonable files, they will be displayed under the Zonable files. | | | | | |
| Software Suggestions Security Change Password Password Recovery | Itest Debition Stattings Itest Debition Stattings Itest Debition Stattings | | | | | |
| | Preters SHS Threaturp This setting determines your preferred Timestamp provider. If you don't need any timestamp provider then select No timestamp required. (2) No timestamp required Mask That That Short Uber Name Mask That That Short Uber Name This setting role tappicable for SCOM imports) is used to ensure windows environment variable names are used instead of user name for the paths that contain profile names. (2) | | | | | |
| | Enable Marking Configure Agents Configure Agents Status Poling After submitting scant to the server, agent polis the server to figure out if the processing is completed. You can reduce the server traffic by stopping agent from poling. (2) Stop agent poling | | | | | |

1

Overview Scan Results Blocked Results Zombie File Results

42 ×

| ame 1 | Version | State | SAID | Path | Criticality | CVSS Ba | Th | Issued | Vulner |
|-------------------------|-------------|--------|------|--|-------------|---------|----|--------|--------|
| licrosoft Visual C++ 20 | 11.0.5072 | Secure | | C:Windows/SysWOW64/msvcr110.dll | | | | 2 | |
| licrosoft Visual C++ 20 | 14.29.301 | Secure | | C /Program Files (x86)/AdminStudio/2022/Repackager/msvcp140.dll | | | | | |
| licrosoft Visual C++ 20 | 14.0.2421 | Secure | | C:\Program Files (x86)\Microsoft Intune Management Extension\msvcp140.dll | | | | | |
| licrosoft Visual C++ 20 | 14.34.319 | Secure | | C /Program Files (x86)/Microsoft/Edge/Application/115.0.1901.188/msvcp140.dll | | | | | |
| licrosoft Visual C++ 20 | 14.34.319 | Secure | | C:/Program Files (x86)/Microsoft/EdgeCore\115.0.1901.188/msvcp140.dll | | | | | |
| licrosoft Visual C++ 20 | 14.34.319 | Secure | | C: \Program Files (x86)/Microsoft/EdgeWebView/Application\115.0.1901.188/msvcp140.dll | | | | | |
| licrosoft Visual C++ 20 | 14.16.270 | Secure | | C 'Program Files (x86)/Mozilla Thunderbird/msvcp140.dll | | | | | |
| licrosoft Visual C++ 20 | 14.28.293 | Secure | | C:\Program Files (x86)\Zoom\bin\aomhost64\msvcp140.dll | | | | | |
| icrosoft Visual C++ 20 | 14.28.293 | Secure | | C:\Program Files (x86)\Zoom\bin\msvcp140.dll | | | | | |
| licrosoft Visual C++ 20 | 14.16.270 | Secure | | C:\Program Files\Mozilla Firefoximsvcp140.dll | | | | | |
| licrosoft Visual C++ 20 | 14.16.270 | Secure | | C:\Program Files\Mozilla Thunderbird\msvcp140.dll | | | | | |
| licrosoft Visual C++ 20 | 14.16.270 | Secure | | C:\Program Files\WindowsApps\Microsoft.Microsoft3DViewer_7.2211.24012.0_x648wekyb3d8bbwe\msvcp140.dll | | | | | |
| licrosoft Visual C++ 20 | 14.29.301 | Secure | 8 | C:\Program Files\WindowsApps\Microsoft.SkypeApp_15.96.3207.0_x64kzf8qxf38zg5c\Skype\msvcp140.dll | | | 1 | 3 | |
| licrosoft Visual C++ 20 | 14.29.301 | Secure | | C:\Program Files\WindowsApps\Microsoft.SkypeApp_15.99.3403.0_x64kzf8qxf38zg5c\Skype\msvcp140.dll | | | | | |
| licrosoft Visual C++ 20 | 14.30.307 | Secure | ÷ | C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00.UWPDesktop_14.0.30704.0_x648wekyb3d8bbwe\msvcp140.dll | | | | - | |
| licrosoft Visual C++ 20 | 14.30.307 | Secure | | C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00.UWPDesktop_14.0.30704.0_x868wekyb3d8bbwe\msvcp140.dll | | | | | |
| icrosoft Visual C++ 20 | 14.32.313 | Secure | | %USERPROFILE%AppDatalLocal/MicrosoftiOneDrive123.061.0319.0003/msvcp140.dll | | | | * | |
| icrosoft Visual C++ 20 | 14.24.281 | Secure | | C:/Windows/System32/msvcp140.dll | | | | | |
| icrosoft Visual C++ 20 | 14.31.311 | Secure | 8 | C:Windows\SysWOW64imsvcp140.dll | | | | | |
| licrosoft Windows Defe | 4.18.1909.6 | Secure | | C:/Program Files/Windows Defender/MsMpEng.exe | | | | | |
| icrosoft Windows Defe | 4.18.2305 | Secure | | C.\ProgramDatal/Microsoft\Windows Defender\Platform\4.18.23050.5-0WsMpEng.exe | | | | | |

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)

Refer "Patch Publisher Enhancements" for changelog.

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-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. |

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/intellectualproperty.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.