

Software Vulnerability Manager (On-Premises Edition) Release Notes

April 2022

Introduction	1
New Features and Enhancements	2
Updated Software Vulnerability Manager User Interface	2
Support for Proxy Settings in SVM Patch Publisher	2
Support for Logged Path in Scan Paths.....	3
Binary Versions Changed.....	4
Known Issues	4
Resolved Issues	5
Community Blogs	5
Product Feedback	5
Legal Information	5

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.

New Features and Enhancements

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

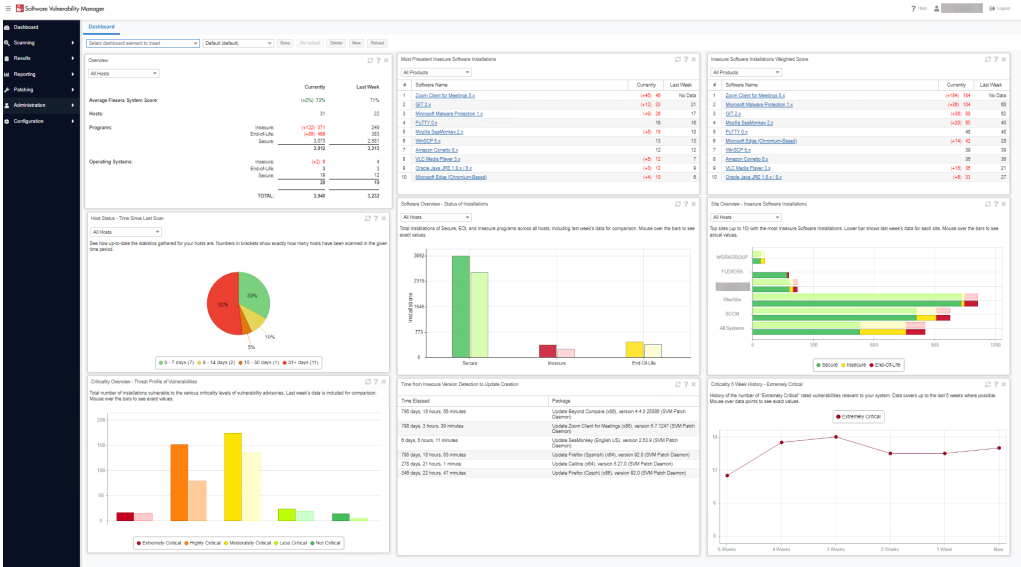
- Updated Software Vulnerability Manager User Interface
- Support for Proxy Settings in SVM Patch Publisher
- Support for Logged Path in Scan Paths
- Binary Versions Changed



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).

Updated Software Vulnerability Manager User Interface

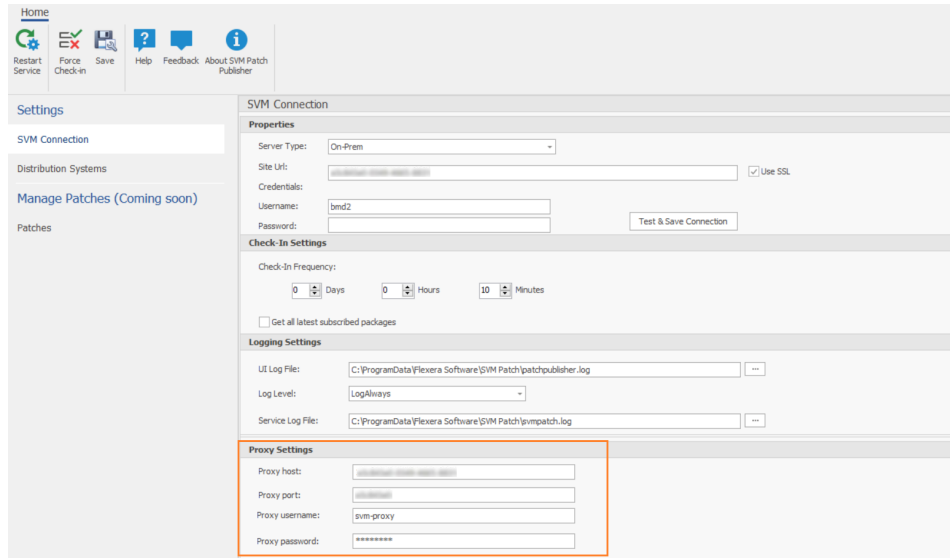
This update presents Software Vulnerability Manager with a new, refreshed and modern user interface. While the overall layout, menu options and their placement in the user interface almost remain the same, there are couple of significant improvements added, like clicking on a menu item opens a new tab within the SVM console for easy navigation and a new URL.



For more details on the new user interface and FAQ, [click here](#).

Support for Proxy Settings in SVM Patch Publisher

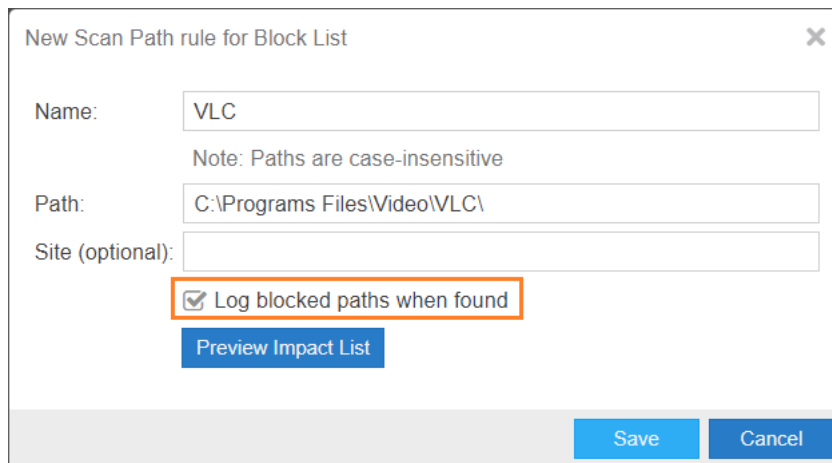
This update allows you to configure a proxy server in the SVM Patch Publisher. When a proxy server is configured, all the communication to the SVM Patch Publisher go through the configured proxy serve.



For more information, see [Configure SVM Patch Publisher Proxy Settings](#).

Support for Logged Path in Scan Paths

When a path is marked as blocked, the SVM scan agent ignores this path for scanning. However, if you wish to log a blocked path for your awareness, then check the new option, available with this update, **Log blocked paths when found** option in the **New Scan Path rule for Block List** dialog.



All the blocked paths which are selected for logging will be set to Yes in the new column named **Logged** in the **Block List** view under the **Scan Paths** menu in the left navigation pane.

Name	Path	Site	Logged
GA	c:\program files\mingw\bin\mingw32.exe		Yes
Mac	%System%\Applications\Utilities\AirPort Utility.app\Contents\Info.plist	MacSite	No
	C:\Program Files\Notepad++		No
One Drive	%LOCALAPPDATA%\Microsoft\OneDrive\OneDrive.exe		Yes
OneDrive	%USERPROFILE%\appData\Local\Microsoft\OneDrive\OneDrive.exe		Yes
Python	%Applications%\Python 3.9\Python Launcher.app\Contents\Info.plist		Yes
	%USERPROFILE%\AppData\Local\Programs\Python\Python35\python35.dll		Yes
User Profile	%USERPROFILE%	Flexera	No

For a given host, all the products associated with the logged blocked paths can be seen under the new tab named **Blocked Results** for the host in the **Completed Scans**.

Name	Version	State	SAID	Criticality	CVSS Base S...	Threat S...	Issued	Vulnerabilities
Amazon Corr...	8.0.2420.8	Insecure	SA106167		v3: 5.3	22	68 days ago	13
Amazon Corr...	8.0.2420.8	Insecure	SA106167		v3: 5.3	22	68 days ago	13
Google Toolb...	4.0.1601.4978	Secure	-			-	-	-
Google Toolb...	7.5.7819.1252	Secure	-			-	-	-
Microsoft Inte...	11.0.9600.190...	Secure	-			-	-	-
Microsoft Inte...	11.0.9600.190...	Secure	-			-	-	-
Microsoft Visu...	14.16.27012.6	Secure	-			-	-	-
Microsoft Visu...	14.16.27012.6	Secure	-			-	-	-
VLC Media PL...	3.0.13.0	Secure	-			-	-	-
Winamp 5 x	5.6.3.3234	Secure	-			-	-	-

Binary Versions Changed

The following version of the binaries provided are:

- SVM ActiveX Plug-in v7.6.1.19 (no change)
- Single Host Agent v7.6.1.19 (no change)
- SVM Daemon v7.6.1.19 (no change)
- SVM System Center Plugin v7.6.1.19 (no change)
- SVM Patch Publisher v6.1.640 (to download, [click here](#))
- SVM On-Prem Client Toolkit v5.0.547 (to download, [click here](#)) (no change)

Known Issues

This release of Software Vulnerability Manager (On-Premises Edition) does not include any known issues.

Resolved Issues

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

Issue	Description
IOJ-2190921	Agents deployed with custom GroupName switches to Site Name on agent check in.
IOJ-2250844	Database Console data export giving invalid token error.
IOJ-2252378	Dashboard showing the status as “loading” and throwing the console error.

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.