Software Vulnerability Manager (Cloud Edition) Release Notes

March 2022

Introduction 1

New Features and Enhancements 1

- **Support for Proxy Settings in SVM Patch Publisher** 2
- **Support for Logged Path in Scan Paths** 2
- **Binary Versions** 4

Known Issues 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 or VMware® Workspace One.

New Features and Enhancements

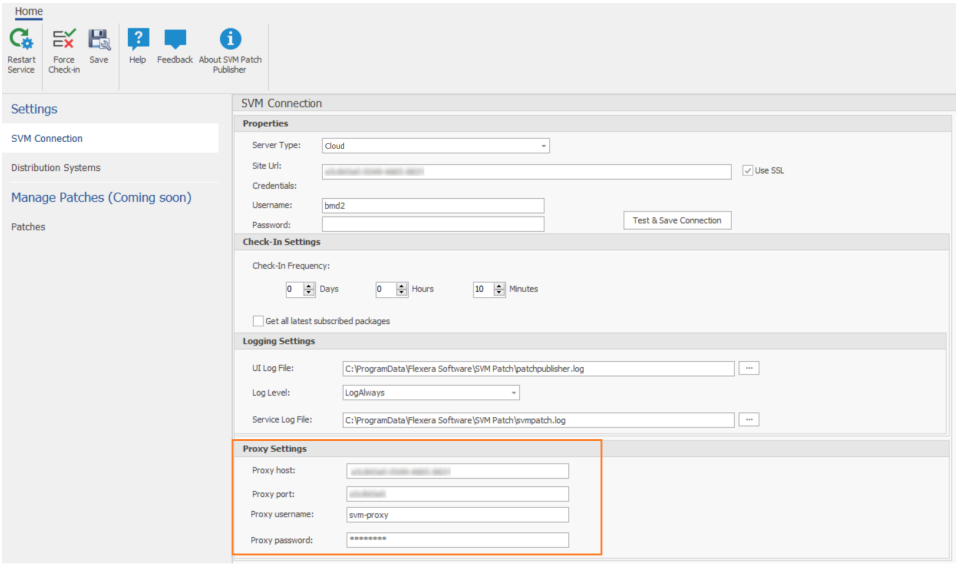
Software Vulnerability Manager (Cloud Edition) includes the following new features and enhancements:

- Support for Proxy Settings in SVM Patch Publisher
- Support for Logged Path in Scan Paths
- 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).*

Support for Proxy Settings in SVM Patch Publisher

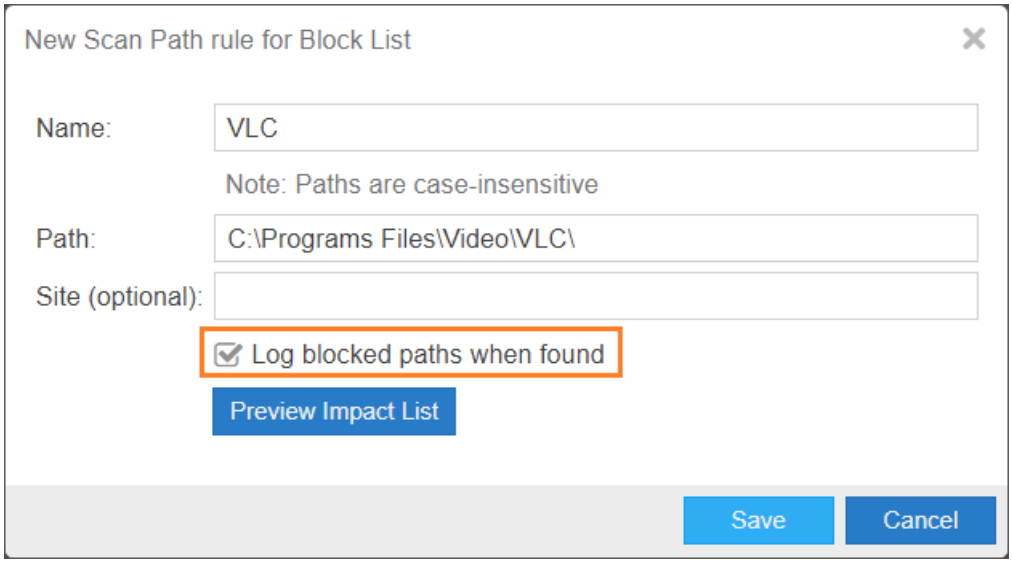
This update allows you to configure a proxy server in the SVM Patch Publisher. When a proxy server is configured, all the communication to the SVM Patch Publisher go through the configured proxy serve.



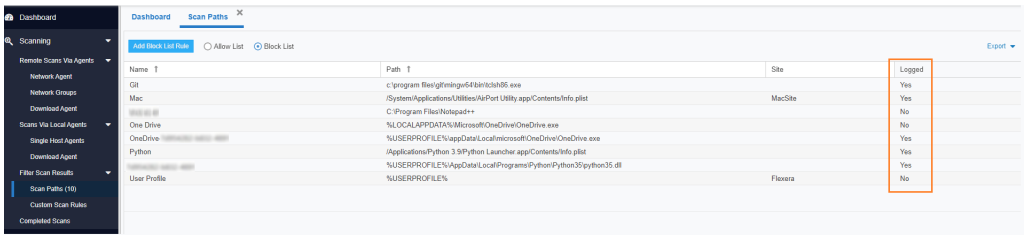
For more information, see Configure SVM Patch Publisher Proxy Settings.

Support for Logged Path in Scan Paths

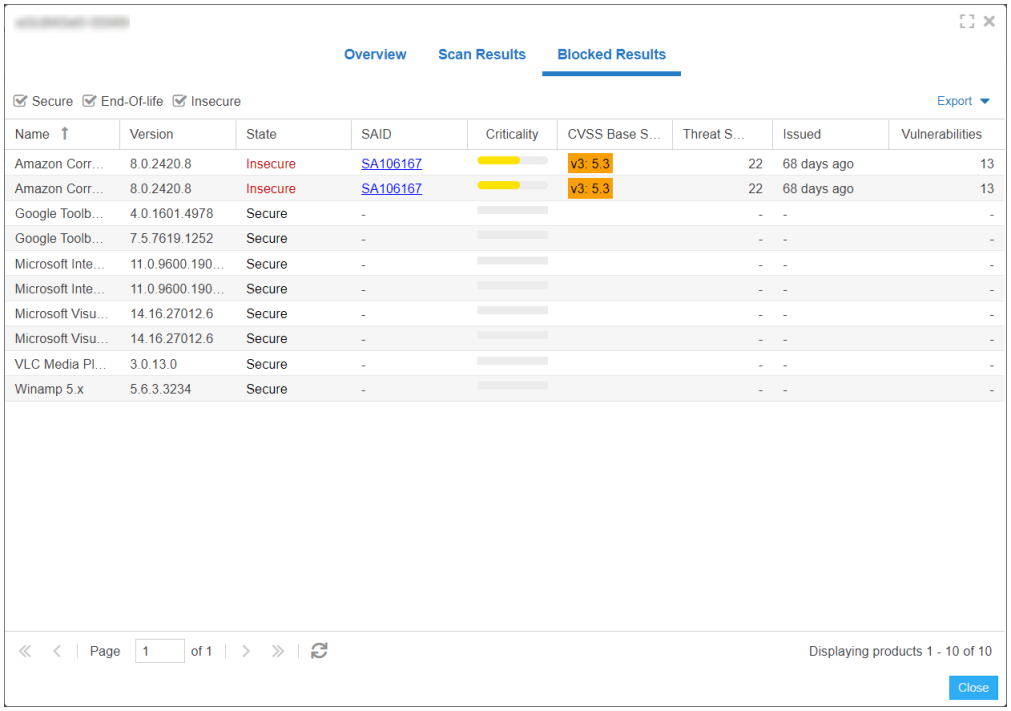
When a path is marked as blocked, the SVM scan agent ignores this path for scanning. However, if you wish to log a blocked path for your awareness, then check the new option, available with this update, **Log blocked paths when found** option in the **New Scan Path rule for Block List** dialog.



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.



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**.



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 v6.1.640 (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.

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

  This toolkit contains Patch Daemon and offline utilities such as the Multi-partition Reporting Tool, WSUS Management Tool and Client Data Tool which add value to SVM.

Known Issues

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

Resolved Issues

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

Issue	Description
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

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.