Software Vulnerability Manager (Cloud Edition) Release Notes

September 2023

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.

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

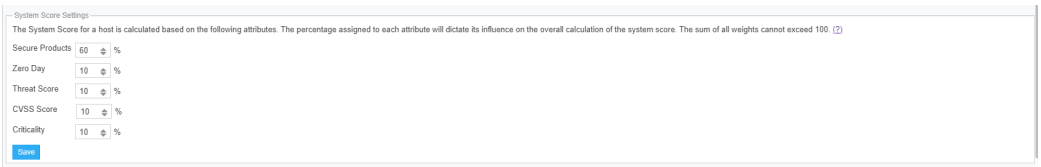
Software Vulnerability Manager (Cloud Edition) includes the following new features and enhancements:

- Flexera System Score Enhancements
- View Scan Result for Hosts/Devices in SVM Patch Publisher
- Reference: Latest Binary Versions

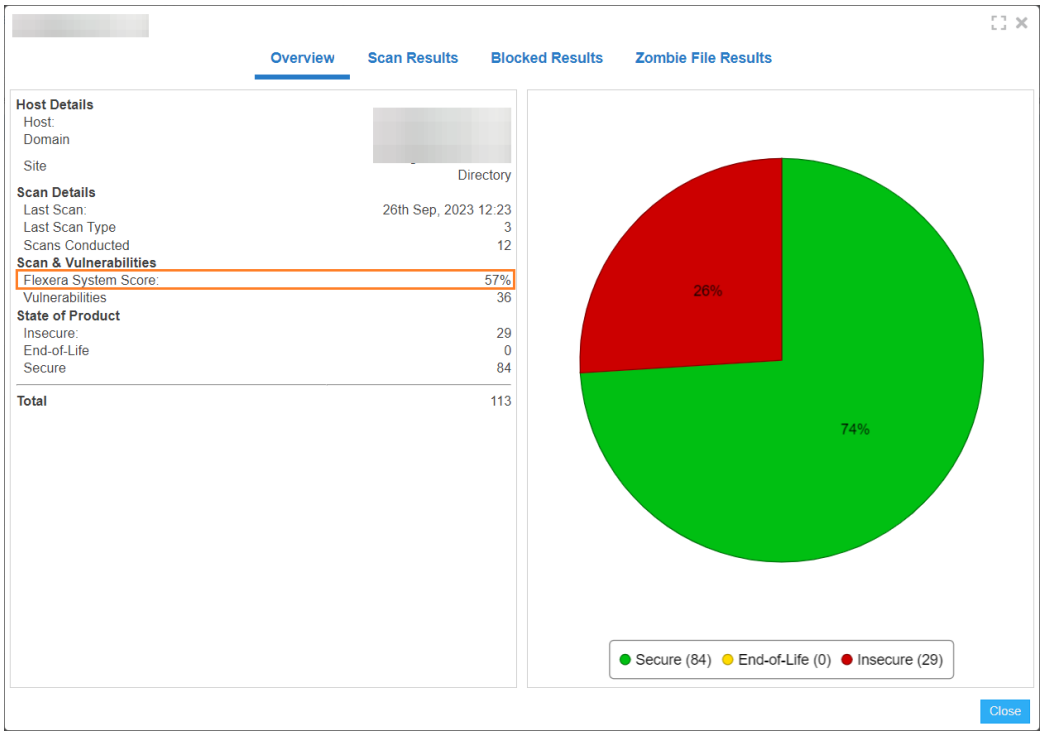
Note • *To see the following new features and enhancements in your Software Vulnerability Manager (Cloud Edition) interface, you must refresh your browser's cache (press Ctrl+F5).*

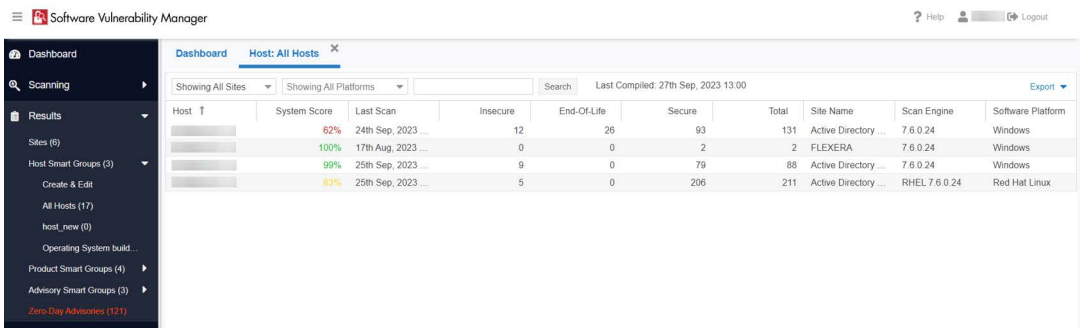
Flexera System Score Enhancements

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.

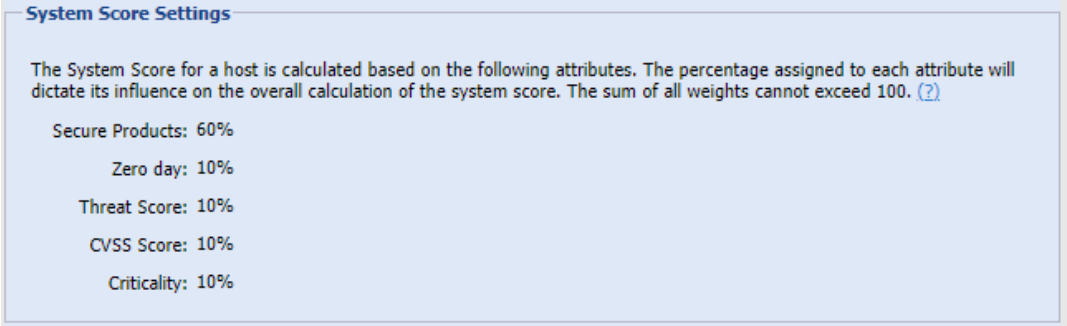


Upon defining the criteria and running the scan, the system score details will be displayed in the **Scanning** > **Completed Scans** > **View Scan Result** > **Overview** tab. Also displayed in the **Host Smart Groups grid**.



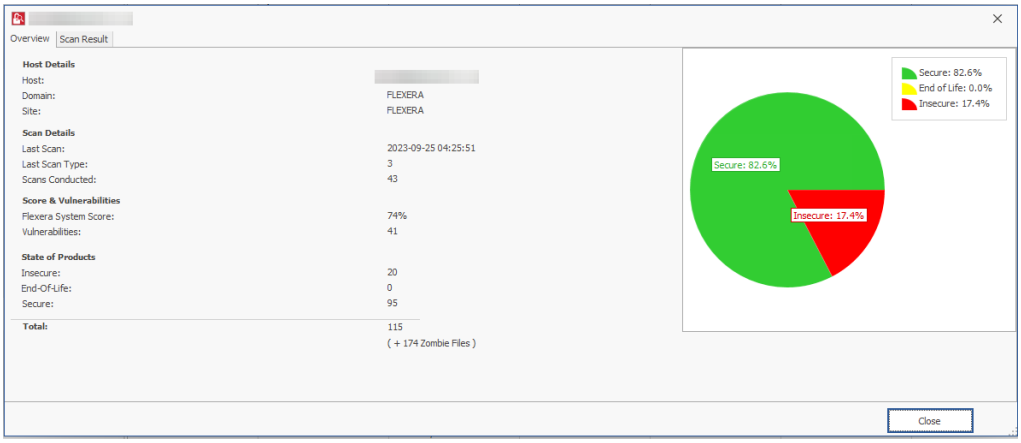


In the old SVM user interface, configured criteria details will be displayed in the **Configuration > Settings > System Score Settings**. These attributes are not editable.



View Scan Result for Hosts/Devices in SVM Patch Publisher

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.



Reference: Latest Binary Versions

The following is the list of binaries versions:

- 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 v7.15.1071 (to download, click here).

  Refer “View Scan Result for Hosts/Devices in SVM Patch Publisher” 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.*

Known Issues

The following table lists the known issues in Software Vulnerability Manager (Cloud Edition):

Issue	Description
IOK-1046547	WSUS Management tool is giving exception when it is relaunched.
IOK-1060172	When certain special characters are used in password, Client Data tool gives “Invalid Token”.

Resolved Issues

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

Issue	Description
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.

Issue	Description
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 the latest posts about Software Vulnerability Manager by going to https://community.flexera.com/t5/Software-Vulnerability/bg-p/SoftwareVulnerabilityManagementblog and clicking **Subscribe**.

Please subscribe to the 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 **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.