Software Vulnerability Manager (Cloud Edition) Release Notes

June 2020

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

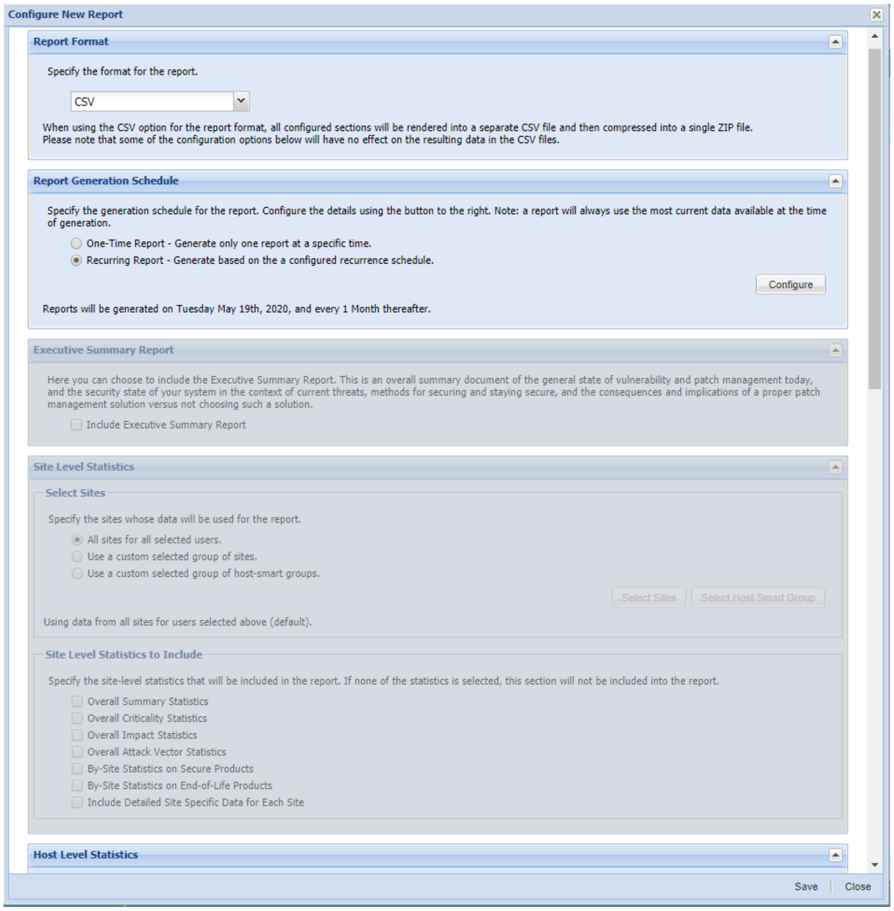
Software Vulnerability Manager (Cloud Edition) includes the following new features and enhancements:

- Disable report options based on report format
- Added CVSS Score to the CSV Reports

***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).*

Disable report options based on report format

With this new enhancement, **Executive Summary Report**, **Dashboard Profiles**, **Site Level Statistics**, and Overall Summary Statistics Check box for both **Host Level Statistics** and **Product Level Statistics** are disabled when you select report format as CSV.



Configure New Report

Report Format

Specify the format for the report.

CSV

When using the CSV option for the report format, all configured sections will be rendered into a separate CSV file and then compressed into a single ZIP file.
Please note that some of the configuration options below will have no effect on the resulting data in the CSV files.

Report Generation Schedule

Specify the generation schedule for the report. Configure the details using the button to the right. Note: a report will always use the most current data available at the time of generation.

○ One-Time Report - Generate only one report at a specific time.
● Recurring Report - Generate based on the a configured recurrence schedule.

Reports will be generated on Tuesday May 19th, 2020, and every 1 Month thereafter.

Executive Summary Report

Here you can choose to include the Executive Summary Report. This is an overall summary document of the general state of vulnerability and patch management today, and the security state of your system in the context of current threats, methods for securing and staying secure, and the consequences and implications of a proper patch management solution versus not choosing such a solution.

□ Include Executive Summary Report

Site Level Statistics

Select Sites

Specify the sites whose data will be used for the report.

● All sites for all selected users.
○ Use a custom selected group of sites.
○ Use a custom selected group of host-smart groups.

Using data from all sites for users selected above (default).

Site Level Statistics to Include

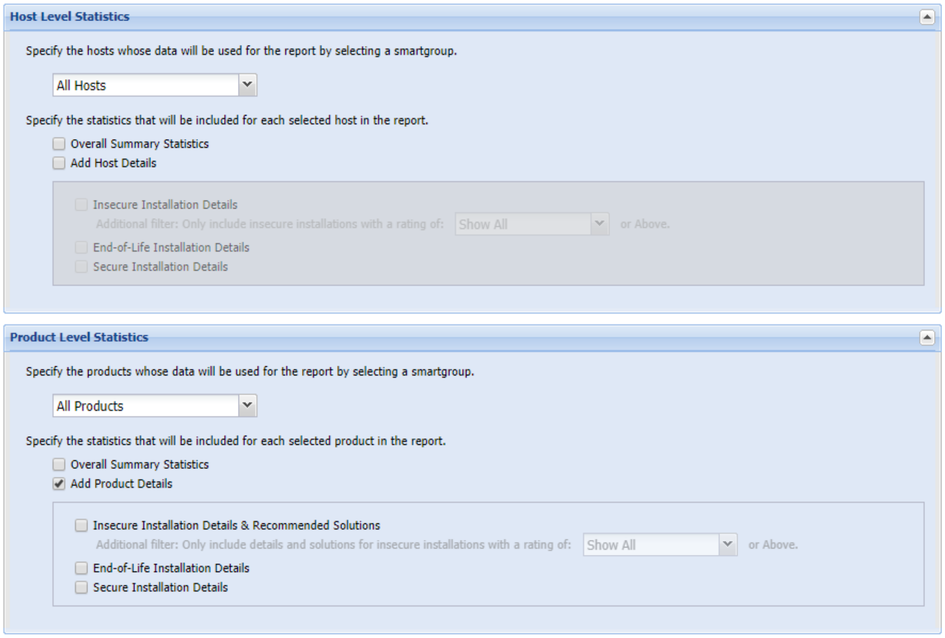
Specify the site-level statistics that will be included in the report. If none of the statistics is selected, this section will not be included into the report.

□ Overall Summary Statistics
□ Overall Criticality Statistics
□ Overall Impact Statistics
□ Overall Attack Vector Statistics
□ By-Site Statistics on Secure Products
□ By-Site Statistics on End-of-Life Products
□ Include Detailed Site Specific Data for Each Site

Host Level Statistics

Figure 1: Select Report as CSV

Insecure Installation Details for both **Host Level Statistics** and **Product Level Statistics** are enabled only when you select **Add Product Details** and **Add Host Details** respectively.



Host Level Statistics

Specify the hosts whose data will be used for the report by selecting a smartgroup.

All Hosts

Specify the statistics that will be included for each selected host in the report.

□ Overall Summary Statistics

□ Add Host Details

□ Insecure Installation Details

Additional filter: Only include insecure installations with a rating of: Show All or Above.

□ End-of-Life Installation Details

□ Secure Installation Details

Product Level Statistics

Specify the products whose data will be used for the report by selecting a smartgroup.

All Products

Specify the statistics that will be included for each selected product in the report.

□ Overall Summary Statistics

☑ Add Product Details

□ Insecure Installation Details & Recommended Solutions

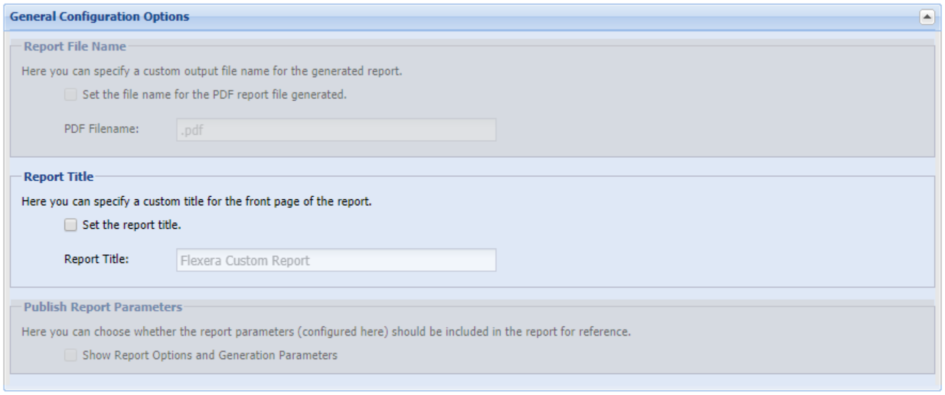
Additional filter: Only include details and solutions for insecure installations with a rating of: Show All or Above.

□ End-of-Life Installation Details

□ Secure Installation Details

Figure 2: Select Add Host Details and Add Product Details respectively

PDF Filename tab and **Publish Report Parameters** sections are disabled when you select report format as CSV.



General Configuration Options

Report File Name

Here you can specify a custom output file name for the generated report.

□ Set the file name for the PDF report file generated.

PDF Filename: .pdf

Report Title

Here you can specify a custom title for the front page of the report.

□ Set the report title.

Report Title: Flexera Custom Report

Publish Report Parameters

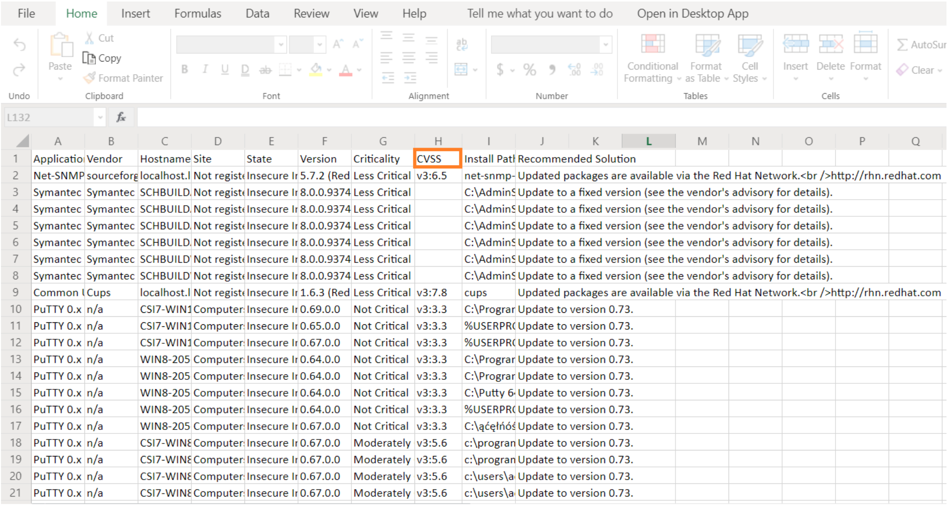
Here you can choose whether the report parameters (configured here) should be included in the report for reference.

□ Show Report Options and Generation Parameters

Figure 3: PDF Filename and Publish Report Parameters fields are Disabled

Added CVSS Score to the CSV Reports

With this new enhancement, a new CVSS column has been added to the CSV Reports.



	A	B	C	D	E	F	G	H	I	J
1	Applicatio	Vendor	Hostname	Site	State	Version	Criticality	CVSS	Install Patl	Recommended Solution
2	Net-SNMP	sourceforg	localhost.l	Not registe	Insecure Ir	5.7.2 (Red	Less Critical	v3:6.5	net-snmp-	Updated packages are available via the Red Hat Network.<br />http://rhn.redhat.com
3	Symantec	Symantec	SCHBUILD.	Not registe	Insecure Ir	8.0.0.9374	Less Critical		C:\AdminS	Update to a fixed version (see the vendor's advisory for details).
4	Symantec	Symantec	SCHBUILD.	Not registe	Insecure Ir	8.0.0.9374	Less Critical		C:\AdminS	Update to a fixed version (see the vendor's advisory for details).
5	Symantec	Symantec	SCHBUILD.	Not registe	Insecure Ir	8.0.0.9374	Less Critical		C:\AdminS	Update to a fixed version (see the vendor's advisory for details).
6	Symantec	Symantec	SCHBUILD.	Not registe	Insecure Ir	8.0.0.9374	Less Critical		C:\AdminS	Update to a fixed version (see the vendor's advisory for details).
7	Symantec	Symantec	SCHBUILD'	Not registe	Insecure Ir	8.0.0.9374	Less Critical		C:\AdminS	Update to a fixed version (see the vendor's advisory for details).
8	Symantec	Symantec	SCHBUILD'	Not registe	Insecure Ir	8.0.0.9374	Less Critical		C:\AdminS	Update to a fixed version (see the vendor's advisory for details).
9	Common U	Cups	localhost.l	Not registe	Insecure Ir	1.6.3 (Red	Less Critical	v3:7.8	cups	Updated packages are available via the Red Hat Network.<br />http://rhn.redhat.com
10	PuTTY 0.x	n/a	CSI7-WIN1	Computer:	Insecure Ir	0.69.0.0	Not Critical	v3:3.3	C:\Prograr	Update to version 0.73.
11	PuTTY 0.x	n/a	CSI7-WIN1	Computer:	Insecure Ir	0.65.0.0	Not Critical	v3:3.3	%USERPR(	Update to version 0.73.
12	PuTTY 0.x	n/a	CSI7-WIN1	Computer:	Insecure Ir	0.67.0.0	Not Critical	v3:3.3	%USERPR(	Update to version 0.73.
13	PuTTY 0.x	n/a	WIN8-205	Computer:	Insecure Ir	0.64.0.0	Not Critical	v3:3.3	C:\Prograr	Update to version 0.73.
14	PuTTY 0.x	n/a	WIN8-205	Computer:	Insecure Ir	0.64.0.0	Not Critical	v3:3.3	C:\Prograr	Update to version 0.73.
15	PuTTY 0.x	n/a	WIN8-205	Computer:	Insecure Ir	0.64.0.0	Not Critical	v3:3.3	C:\Putty 6	Update to version 0.73.
16	PuTTY 0.x	n/a	WIN8-205	Computer:	Insecure Ir	0.64.0.0	Not Critical	v3:3.3	%USERPR(	Update to version 0.73.
17	PuTTY 0.x	n/a	WIN8-205	Computer:	Insecure Ir	0.67.0.0	Not Critical	v3:3.3	C:\ąćęłńóś	Update to version 0.73.
18	PuTTY 0.x	n/a	CSI7-WIN8	Computer:	Insecure Ir	0.67.0.0	Moderately	v3:5.6	c:\progran	Update to version 0.73.
19	PuTTY 0.x	n/a	CSI7-WIN8	Computer:	Insecure Ir	0.67.0.0	Moderately	v3:5.6	c:\progran	Update to version 0.73.
20	PuTTY 0.x	n/a	CSI7-WIN8	Computer:	Insecure Ir	0.67.0.0	Moderately	v3:5.6	c:\users\a	Update to version 0.73.
21	PuTTY 0.x	n/a	CSI7-WIN8	Computer:	Insecure Ir	0.67.0.0	Moderately	v3:5.6	c:\users\a	Update to version 0.73.

Figure 4: Added CVSS Column in CSV Reports

Resolved Issues

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

Issue	Description
IOJ-2098888	Enhanced Advisories smart group grids to search with SAID and Advisory Description. CVE Search already available.
IOJ-2118632	Fixed email not triggering after completing external package signature.

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.