

Software Vulnerability Manager (On-Premises Edition) Release Notes

August 2020

Introduction	1
New Features and Enhancements	2
Single Sign-On (SSO)	2
External Package Signing for Software Vulnerability Manager Client Toolkit.....	2
Disable Report Options Based on Report Format.....	3
Added CVSS Score to the CSV Reports	5
Search Advisory by SAID	5
Binary Versions	6
Resolved Issues	6
Community Blogs	6
Product Feedback	6
Legal Information	7

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:

- [Single Sign-On \(SSO\)](#)
- [External Package Signing for Software Vulnerability Manager Client Toolkit](#)
- [Disable Report Options Based on Report Format](#)
- [Added CVSS Score to the CSV Reports](#)
- [Search Advisory by SAID](#)
- [Binary Versions](#)



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).

Single Sign-On (SSO)

With this release, Software Vulnerability Manager can now support Single Sign On (SAML2 protocol).

This feature will enable the users to authenticate with Identity Provider (IdP) like Okta within your organization.

To configure this feature go to **Configuration > Settings**.

Single Sign-On can be enabled from the **Configuration > Settings** page.

Service Provider Configuration

SSO Enabled (?)

Disable standard login (Ensure SSO is working first, to prevent lockout.)

Provide IDP Metadata URL

Upload IDP Metadata XML file

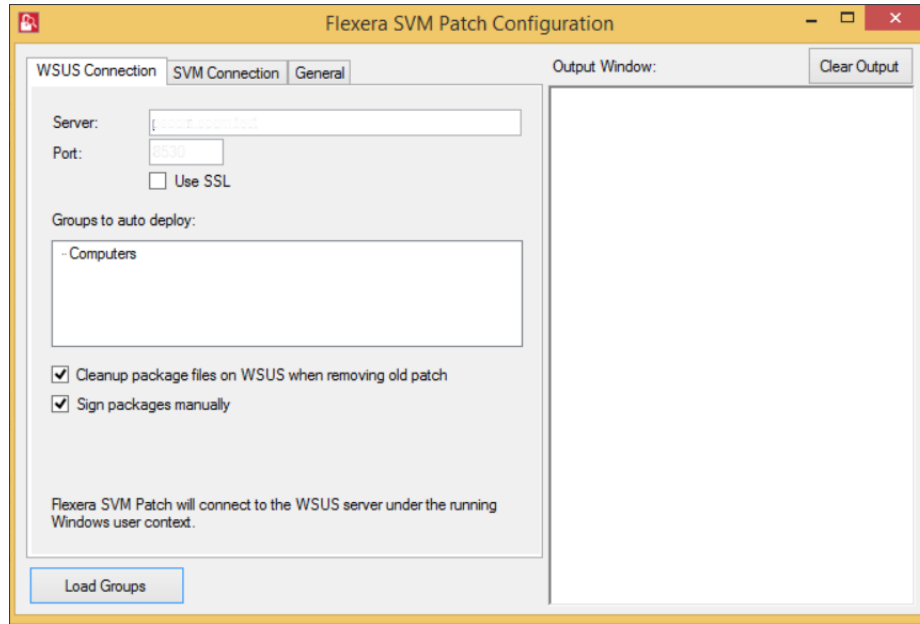
Automatically create new user

For more details, see [Configure Single Sign-On \(SSO\)](#).

External Package Signing for Software Vulnerability Manager Client Toolkit

Using Manual Signatures (also known as External Signatures) allows separating the privilege of Windows Server Update Services (WSUS) administration from the privilege to mark a package as trusted for deployment. With automatic signatures (typically, but not always, using a self-signed certificate), the WSUS administrator has full access to a digital certificate and private key that is trusted by all the machines within the organization. With Manual signatures, WSUS, and thus the WSUS administrator, does not require access to the private key.

In Software Vulnerability Manager Client Toolkit, select **Sign package manually** option.



For detail on performing the Manual package Signing, see [External package signing for Software Vulnerability Manager Client Toolkit](#).

Disable Report Options Based on Report Format

With this new enhancement, **Executive Summary Report**, **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.

Configure

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.

Select Sites | Select Host Smart Group

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

Save | Close

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.

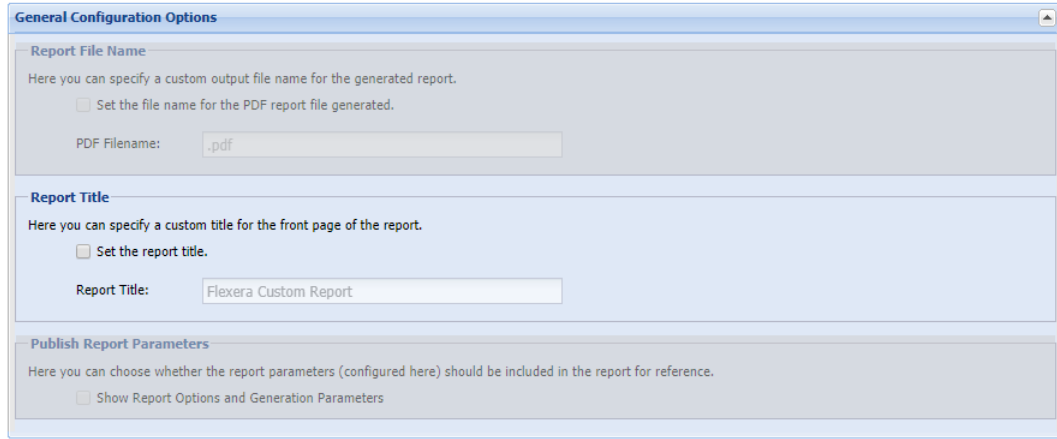
All Products

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

The **PDF Filename** tab and the **Publish Report Parameters** sections are disabled when you set **Report Format** to **CSV**.



Added CVSS Score to the CSV Reports

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

File	Home	Insert	Formulas	Data	Review	View	Help	Tell me what you want to do		Open in Desktop App	
1	Application Vendor	Hostname Site	State	Version	Criticality	CVSS		Install Patch Recommended Solution			
2	Net-SNMP	sourceforge	localhost:1	Not regist	Insecure Ir 5.7.2 (Red)	Less Critical	v3:6.5	net-snmp- Updated packages are available via the Red Hat Network. -/http://rhn.redhat.com			
3	Symantec	Symantec	SCHBUILD	Not regist	Insecure Ir 8.0.0.9374	Less Critical		C:\Admin\$ Update to a fixed version (see the vendor's advisory for details).			
4	Symantec	Symantec	SCHBUILD	Not regist	Insecure Ir 8.0.0.9374	Less Critical		C:\Admin\$ Update to a fixed version (see the vendor's advisory for details).			
5	Symantec	Symantec	SCHBUILD	Not regist	Insecure Ir 8.0.0.9374	Less Critical		C:\Admin\$ Update to a fixed version (see the vendor's advisory for details).			
6	Symantec	Symantec	SCHBUILD	Not regist	Insecure Ir 8.0.0.9374	Less Critical		C:\Admin\$ Update to a fixed version (see the vendor's advisory for details).			
7	Symantec	Symantec	SCHBUILD	Not regist	Insecure Ir 8.0.0.9374	Less Critical		C:\Admin\$ Update to a fixed version (see the vendor's advisory for details).			
8	Symantec	Symantec	SCHBUILD	Not regist	Insecure Ir 8.0.0.9374	Less Critical		C:\Admin\$ Update to a fixed version (see the vendor's advisory for details).			
9	Common (Cups	localhost:1	Not regist	Insecure Ir 1.6.3 (Red)	Less Critical	v3:7.8		cups Updated packages are available via the Red Hat Network. -/http://rhn.redhat.com			
10	PuTTY 0.x	n/a	CS17-WIN1	Computer:	Insecure Ir 0.69.0.0	Not Critical	v3:3.3	C:\Program Update to version 0.73.			
11	PuTTY 0.x	n/a	CS17-WIN1	Computer:	Insecure Ir 0.65.0.0	Not Critical	v3:3.3	%USERPRK Update to version 0.73.			
12	PuTTY 0.x	n/a	CS17-WIN1	Computer:	Insecure Ir 0.67.0.0	Not Critical	v3:3.3	%USERPRK 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:\Program 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:\Program 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	%USERPRK 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:\ççññó Update to version 0.73.			
18	PuTTY 0.x	n/a	CS17-WIN1	Computer:	Insecure Ir 0.67.0.0	Moderately	v3:5.6	c:\program Update to version 0.73.			
19	PuTTY 0.x	n/a	CS17-WIN1	Computer:	Insecure Ir 0.67.0.0	Moderately	v3:5.6	c:\program Update to version 0.73.			
20	PuTTY 0.x	n/a	CS17-WIN1	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	CS17-WIN1	Computer:	Insecure Ir 0.67.0.0	Moderately	v3:5.6	c:\users\%a Update to version 0.73.			

Search Advisory by SAID

With this new enhancement, you can search Advisory either by **CVE**, **SAID**, or **Description**.

Search Type	CVE	Search	Export							
SAID	CVE	Criticality	Threat Sc...	Zero-Day	Advisory Published	Vulnerabilit...	Solution Status	CVSS Base Score	CVSS2 Base Score	CVSS3 Base S
SA82501	SAID			No	10th Apr, 2018	6	Vendor Patched	v2: 10	v3: 4.4	10
SA80014	Description			No	14th Nov, 2017	5	Vendor Patched	v2: 10	v3: 10	10
SA81606	Adobe...			No	13th Feb, 2018	41	Vendor Patched	v2: 10	v3: 8.8	10
SA80028	Adobe...			No	14th Nov, 2017	1	Vendor Patched	v2: 10	v3: 8.8	10
SA79744	Apach...			No	27th Oct, 2017	4	Vendor Patched	v2: 10	v3: 10	10
SA82242	Apple...			No	30th Mar, 2018	17	Vendor Patched	v2: 10	v3: 8.8	10
SA34799	eMule...			No	21st Apr, 2009	1	Vendor Patched			0

Binary Versions

The following are the new version of the binaries provided for this release:

Binaries version: 7.6.1.13

Resolved Issues

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

Issue	Description
IOJ-2125934	Renamed White/Black List Feature to Allow list/Block list.
IOJ-1865237	The smart group drop-down is removed for Criticality Overview - Threat Profile of Vulnerabilities dashboard.
IOJ-2129915	LDAPS password enhancement requests.

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 © 2020 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.