Software Vulnerability Manager (On-Premises Edition) Release Notes

August 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 (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.

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.
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.
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.

---

**Search Advisory by SAID**

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

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

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.