Software Vulnerability Manager 2019 R3 (On-Premises Edition) Release Notes

July 2019

Introduction

Flexera's Software Vulnerability Manager 2019 is a Vulnerability and Patch Management Software Solution that facilitates a customized Patch Management process. It combines Vulnerability Intelligence, Threat 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 2019, IT Operations and Security Teams are empowered to prevent vulnerability threats from both Microsoft and non-Microsoft (third-party) product vulnerabilities, covering Microsoft Windows, Mac OS, and Red Hat Enterprise Linux.

Software Vulnerability Manager 2019 integrates seamlessly with Microsoft® WSUS and System Center Configuration Manager.

New Features and Enhancements

Software Vulnerability Manager 2019 R3 (On-Premises Edition) includes the following new features and enhancements:

- Vendor Patch Module
- API Support
- New Login Screen
- Signed Agents
- Vendor Patch Module Via SCCM Plug-in
- Agent Scan Start Randomization
- CVSS 2 and CVSS 3 in Product Smart Groups
- CVSS 2 and CVSS 3 in Advisories Smart Groups

Note • *To see the following new features and enhancements in your Software Vulnerability Manager 2019 interface, you must refresh your browser's cache (press Ctrl+F5).*

Vendor Patch Module

In Software Vulnerability Manager 2019 R3, you can find the new feature Vendor Patch Module in **Patching >> Vendor Patch Module**.

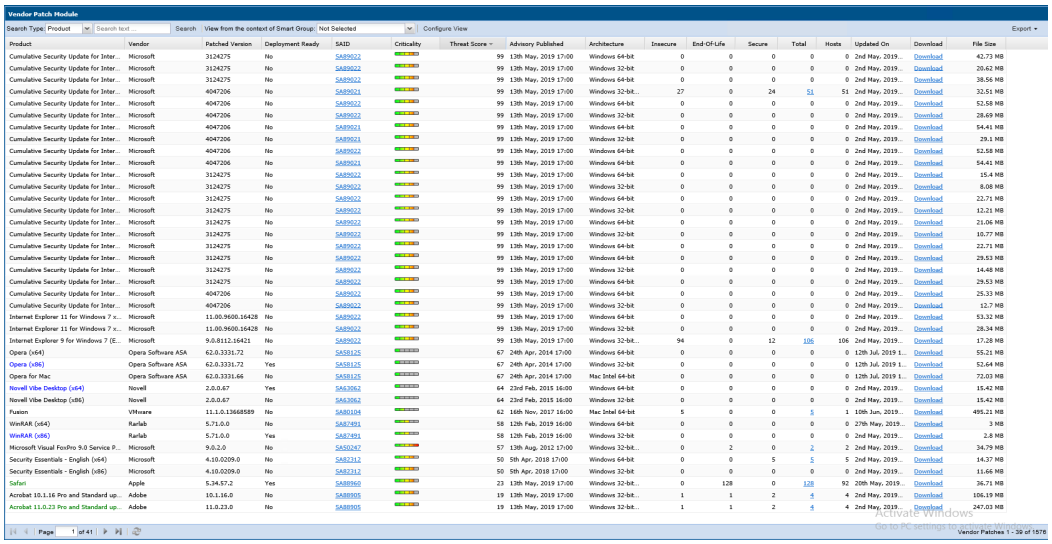
Vendor Patch Module represents the largest set of patch data on the market today. It is designed to integrate over a thousand out of the box patches for prioritization and publishing within SVM. Additionally, it exposes details on over a thousand other vendor setups, which helps you to be aware what patches exist, and to provide as much detail as possible to make bringing your own patch to SVM easier. These additional entries are typically missing something like the actual setup file (because the vendor does not make it publicly available) or because we don't have default applicability criteria (but can leverage assessment results for your environment).

To learn more about the Vendor Patch Module:

- For blog, click here.
- For video, click here.

Important • *Vendor Patch Module is an optional feature and must be purchased separately:*

- *For pricing and availability, please contact your sales representative or contact us online at: https://www.flexera.com/about-us/contact-us.html*
- *If the feature is not purchased, you can view the list of available patches but cannot use them.*



In the Vendor Patch Module products list, you can find the below color codes are used to highlight the completeness of the out of the box patches:

- **Blue color patches** - Out of the box patches are ready to deploy with no missing details, so no extra details needed to deploy these patches.
- **Black color patches** - Patches that are missing some information, but are available to download. To create a patch, any missing details must be provided.
- **Gray color patches** - Patches that are missing some information including the vendor setup files. To create a patch, the vendor setup must be provided along with any missing details.
- **Green color patches** - Patches for which packages have already been created.

Note • *In Software Vulnerability Manager 2019 R3 note the following:*

- *Vendor Patch Module also provides a list of MAC OS patches, You can easily download them for deployment in your Mac management solution of choice.*
- *Vendor Patch Module is now available in SCCM 2012 Plug-in see Vendor Patch Module Via SCCM Plug-in*

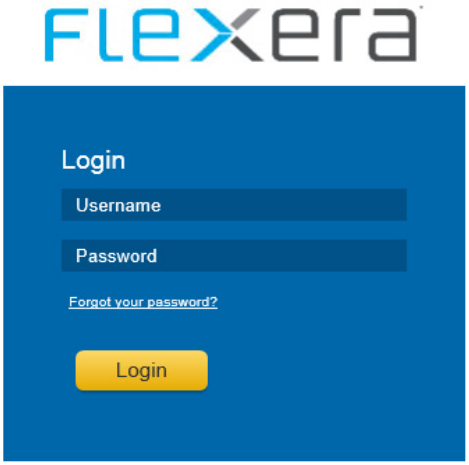
API Support

In Software Vulnerability Manager 2019 R3, API Support is now documented allowing you to integrate SVM 2019 with other systems and processes as well as to pull data for the creation of custom reports.

To learn more about the API document, click here.

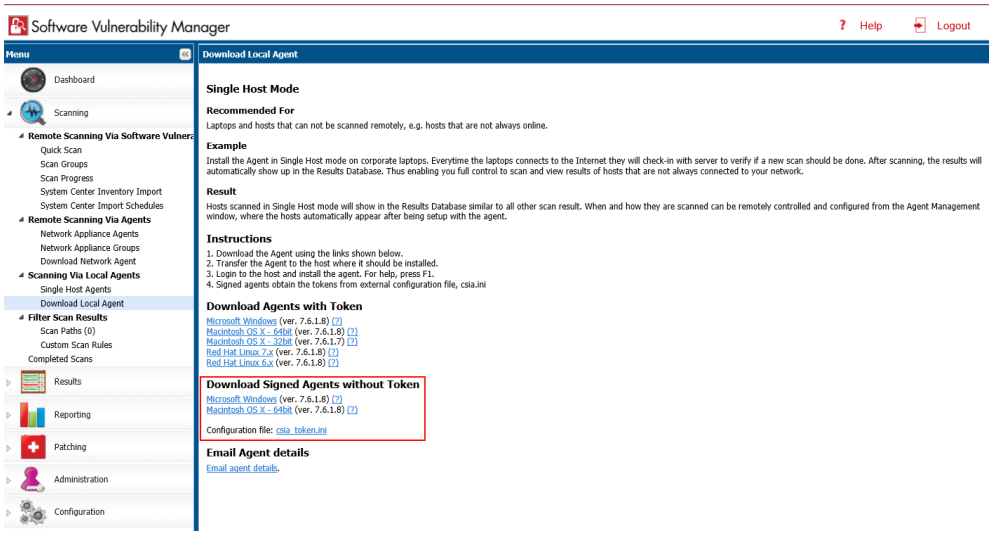
New Login Screen

In Software Vulnerability Manager 2019 R3, you can see the new Login screen as shown below:



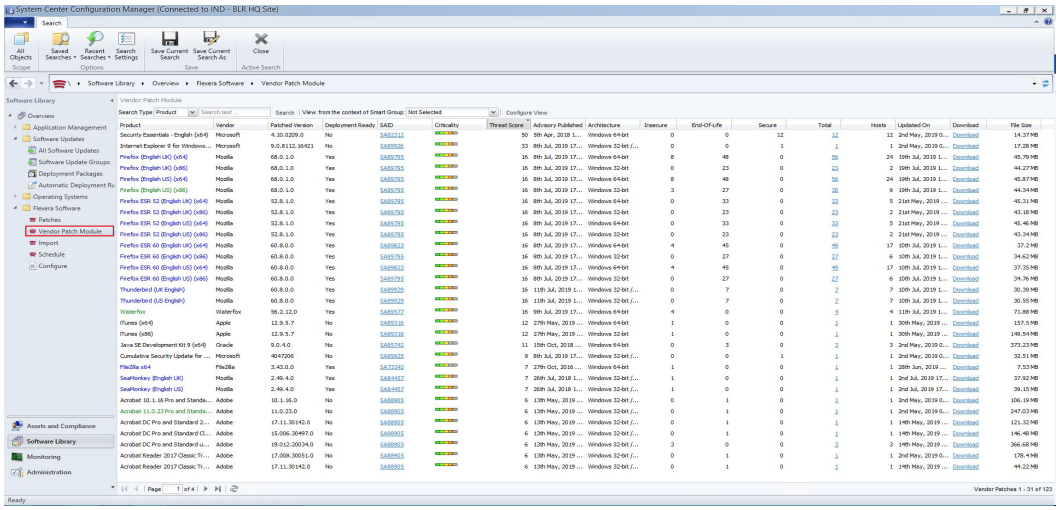
Signed Agents

In Software Vulnerability Manager 2019 R3, you can see the new Signed Agents added in the **Scanning >> Scanning Via Local Agents >> Download Local Agent** as shown below (CSIL-9247):



Vendor Patch Module Via SCCM Plug-in

In Software Vulnerability Manager 2019 R3, you can access the Vendor Patch Module via SCCM 2012 Plugin as shown below (CSIL-9321):



Agent Scan Start Randomization

In Software Vulnerability Manager 2019 R3, maximum randomization of **Agent Scan Start** could be set to 120 min (CSIL-9258).

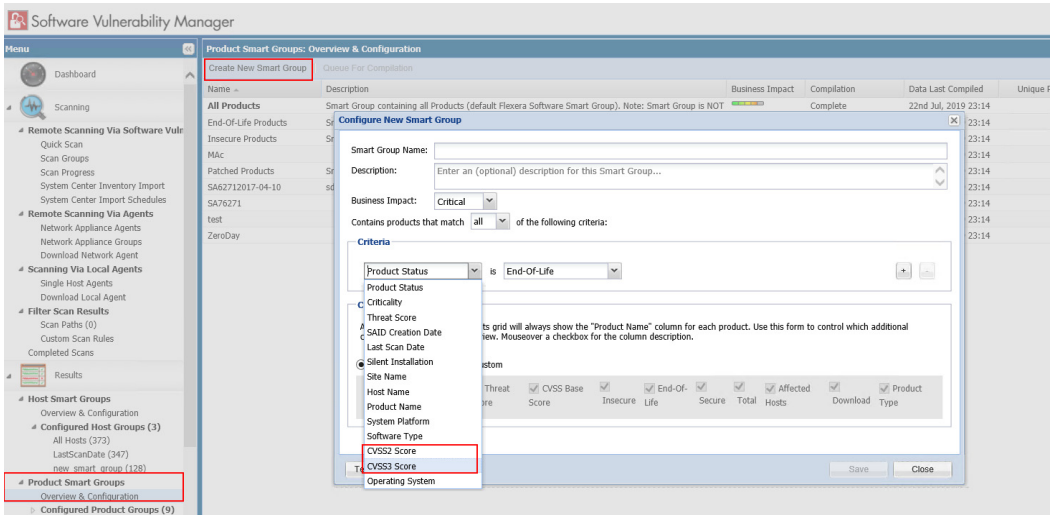
CVSS 2 and CVSS 3 in Product Smart Groups

In Software Vulnerability Manager 2019 R3, you can add CVSS 2 and CVSS 3 as a separate criteria while configuring New Product Smart Group (CSIL-9195):

To create a New Product Smart Groups, select the **Results >> Product Smart Groups >> Overview & Configuration**. List of existing smart group appears.

Click **Create New Smart Group** button. **Configure New smart Group** wizard appears.

In the Criteria section, you can add CVSS 2 and CVSS 3 score as shown below:



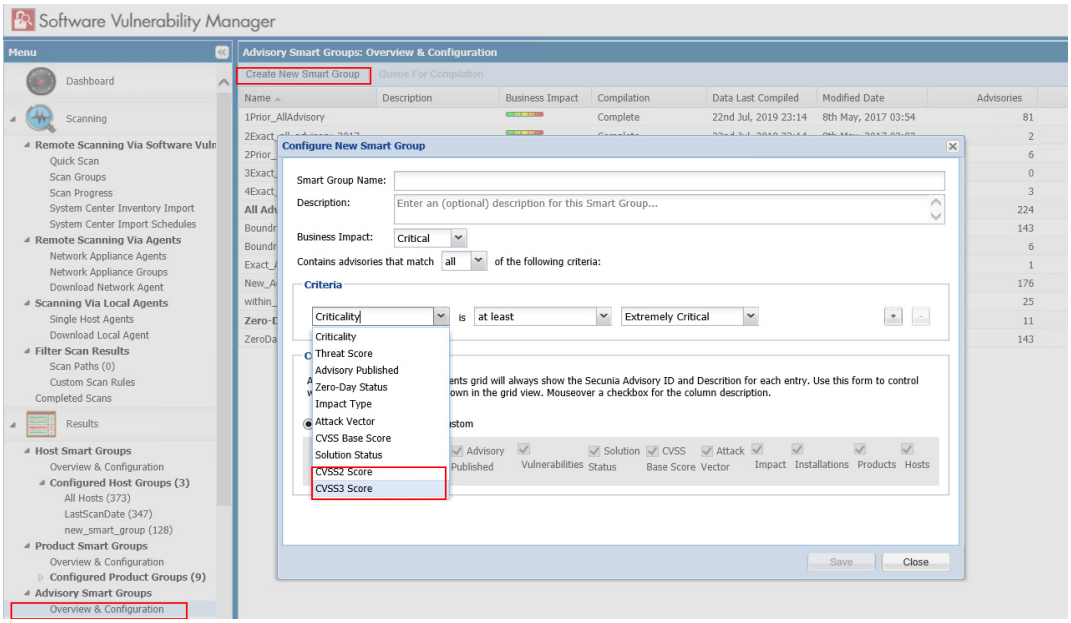
CVSS 2 and CVSS 3 in Advisories Smart Groups

In Software Vulnerability Manager 2019 R3, you can add CVSS 2 and CVSS 3 as a separate criteria while configuring New Adisory Smart Group (CSIL-9195):

To create a New Advisory Smart Groups, select the **Results >> Advisory Smart Groups >> Overview & Configuration**. List of existing smart group appears.

Click **Create New Smart Group** button. **Configure New smart Group** wizard appears.

In the **Criteria** section, you can add CVSS 2 and CVSS 3 score as shown below:



Resolved Issues

The following table lists the customer issues that were resolved in Software Vulnerability Manager 2019 R3:

Issue	Description
IOJ-1923675	HTTP 500 error when Export SPS in Grouped View
IOJ-1912164	Change Download Link column in SVM
IOJ-1890485	Zombie file count is not exported in CSV exports
IOJ-1891404	Product Smart group: "Not in" Clause for selecting Operating System is not working as expected
IOJ-1890428	In Custom Host smart group, counters beside the section is not updating after successful deletion
IOJ-1879230	Single host agent count is inconsistent

Issue	Description
IOJ-1917907	Report showing garbage in TOC
IOJ-1927629	Conflicting Product SG Criteria Cause SG Compilation Failures, DB Errors (+possible side effects)
IOJ-1986687	Incorrect Office 365 ProPlus vulnerability statuses reported by SVM 2019 R2
IOJ-1928554	Upgrading Apache to latest version in virtual appliance

Product Feedback

Have a suggestion for how we can improve this product? Please come share direct feedback with the product team and vote on ideas submitted by other users in our online community at https://flexeracommunity.force.com/customer/ideas/ideaList.apexp.

System Requirements

To use the Software Vulnerability Manager 2019 console, your system should meet the following requirements:

- Minimum resolution: 1280x1024
- Internet Explorer 11 or higher (Scan results can also be viewed from other browsers)
- Internet connection capable of connecting to https://csi7.secunia.com
- The following addresses should be white-listed in the Firewall/Proxy configuration:
  - crl.verisign.net
  - crl.thawte.com
  - http://crl3.digicert.com
  - http://crl4.digicert.com
  - http://*.ws.symantec.com
  - https://*.secunia.com/
  - http://*.symcb.com
  - http://*.symcd.com
- First-Party cookie settings at least to Prompt (in Internet Explorer)
- Allow session cookies
- A PDF reader

Legal Information

Copyright Notice

Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see https://www.flexera.com/producer/company/about/intellectual-property/. 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.