Software Vulnerability Manager 2019 R1 (Cloud Edition) Release Notes

February 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, 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 it enables 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 R1 (Cloud Edition) includes the following new features and enhancements:

- Support Type 1 scanning for SCCM imports
- Making Session cookies more secure
- Add timeout for Windows Update Agent (WUA) calls
- Daemon to scan Active Directory right after install

***Note** • To see the following new features and enhancements in your Software Vulnerability Manager 2019 interface, you must refresh your browser’s cache.*

Support Type 1 scanning for SCCM imports

SCCM Imports now support Type 1 scans via ActiveX or the Daemon (CSIL-8924).

To enable this advanced feature, edit the following registry keys:

- For the Daemon, you can specify the inspection type using the **-t** command line parameter or the Daemon registry key: `[HKEY_CURRENT_USER\Software\Secunia\Daemon]"InspectionType" = dword:00000001`
- For ActiveX, you can specify the inspection type using the CSI Plugin registry key: `[HKEY_CURRENT_USER\Software\Secunia\CSI Plugin]"InspectionType" = dword:00000001`

Making Session cookies more secure

Session cookies have been made secure by adding HTML only and secure attributes (CSIL-8957).

Add timeout for Windows Update Agent (WUA) calls

The SVM agent has a new time-out mechanism that enables one to configure a time-out period for WUA searches. This option prevents the SVM agent from being stuck waiting for the WUA service to return with data. The default timeout is 30 minutes and is configurable via the -- wua-timeout option. A value of zero means the SVM agent will wait indefinitely for the WUA call to respond back (CSIL-9002).

Example: `csia.exe –I –L – wua-timeout 5`

Daemon to scan Active Directory right after install

When Active Directory (AD) is enabled and the settings to scan the AD are set to the "Daily" frequency, the daemon runs the first scheduled scan after 24 hours. This setup could in some situations lead to the creation of duplicate hosts, if hosts have been moved to a different AD branch. With this release, the daemon will initiate the AD scan as soon as it is installed (CSIL-8994).

Resolved Issues

Software Vulnerability Manager 2019 R1 (Cloud Edition) has resolved the following issues:

- Resolved user deletion issue
- Resolved database cleanup functionality
- Resolved saving of SMS setting in Smart Group Notification
- Resolved display of Users with restricted permission
- Removed trailing spaces from Blacklist/Whitelist path when saving
- Resolved display of Nordic characters in data export
- Resolved handling of space in domain name for Mac agents

Resolved user deletion issue

Users created after the Software Vulnerability Manager 2018 R5 upgrade could not be deleted due to missing the `root_account_id` in the accounts table. This issue has been resolved. Support will provide an "updated" SQL for those customers with existing issues (CSIL-8959).

Resolved database cleanup functionality

The cleanup rule was not deleting very old hosts. This issue has been resolved (CSIL-8814).

Resolved saving of SMS setting in Smart Group Notification

Even though the Short Message Service (SMS) setting was saved properly in the database, it did not display correctly on the web page, and it always showed the checkbox for default recipients as checked. This issue has been resolved (CSIL-8808).

Resolved display of Users with restricted permission

Restricted Users were being displayed as Read only in the User management module. This issue has been resolved (CSIL-884).

Removed trailing spaces from Blacklist/Whitelist path when saving

Trailing spaces entered by users while saving Blacklist/Whitelist paths led to agents ignoring these paths as they could not match the actual paths on the host machines. This issue has been resolved by ensuring that trailing spaces are removed before saving the data to the database (CSIL-9008).

Resolved display of Nordic characters in data export

Nordic characters were not properly displayed in CSV files. This issue has been resolved (CSIL-8900).

Resolved handling of space in domain name for Mac agents

Mac agents could not post scan data to servers if the host domain names contained spaces. In such cases, the agent reported “`400=>Http/1.1 400 Bad Request`”. This issue has been resolved (CSIL-9051).

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.