Software Vulnerability Manager 2018 R4 (Cloud Edition)

(formerly Corporate Software Inspector)

Release Notes

August 2018

Introduction 1

New Features and Enhancements 2

- Search patch updates by CVE 2
- Additional date fields added to Flexera Package System (SPS) 2
- Revert to last successful scan after Windows scan failure 3
- Agent now supports recovery settings 4

Resolved Issues 4

- No SAID listings for End-of-Life products 5
- Time-out span for patching has increased from 60 to 180 seconds 5
- Silent parameter and user added paths are retained for the SPS wizard 5
- "Patched" is now labeled "Secure" 5
- Whitelisting personal IP addresses 6
- Polish special characters now appear in installation file paths for exported CSV reports 6
- Dashboard option for Smart Groups has been removed 6
- Issue with site reporting 6
- Connecting to the SCCM data for import scan using TLS 1.2 7
- Mac OS X Agent listing of application metadata after scanning 7

Product Feedback 7

System Requirements 7

Legal Information 8

Introduction

Flexera's Software Vulnerability Manager 2018 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 2018, 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 2018 integrates seamlessly with Microsoft® WSUS and System Center Configuration Manager.

New Features and Enhancements

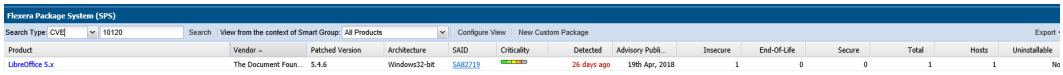
Software Vulnerability Manager 2018 R4 (Cloud Edition) includes the following new features and enhancements:

- Search patch updates by CVE
- Additional date fields added to Flexera Package System (SPS)
- Revert to last successful scan after Windows scan failure
- Agent now supports recovery settings

***Note** • To see the following new features and enhancements in your Software Vulnerability Manager 2018 interface, you must refresh your browser's cache.*

Search patch updates by CVE

In the **Patching > Flexera Package System (SPS) Search by Type** field, you can now search patch updates by Common Vulnerabilities and Exposures (CVE), which are referenced in Secunia Advisories. The CVE results help identify affected hosts, advisories, and patches across entire organizations (CSIL-8408). For the online reference, see Patch update searches by Common Vulnerabilities and Exposures (CVE).



Additional date fields added to Flexera Package System (SPS)

The **Advisory Published** date is now listed in the Patching module under **Flexera Package System (SPS)** for both the grouped and ungrouped views. This date provides a quick reference for the latest patching information (CSIL-8546). For the online reference, see Advisory Published Date.

***Note** • In the Flexera Package System (SPS) ungrouped view which lists each product version separately, there will be no Secunia Advisory IDs (SAID) listed for End-of-Life (EOL) products. Therefore, the Advisory Published date will be blank for EOL products.*

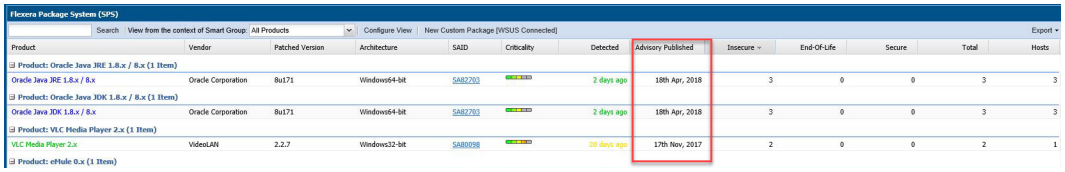


Figure -1: Flexera Package System (SPS) ungrouped view

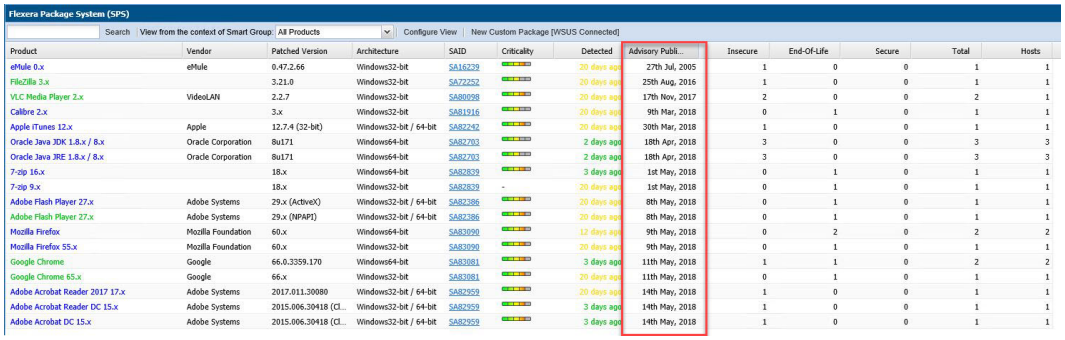
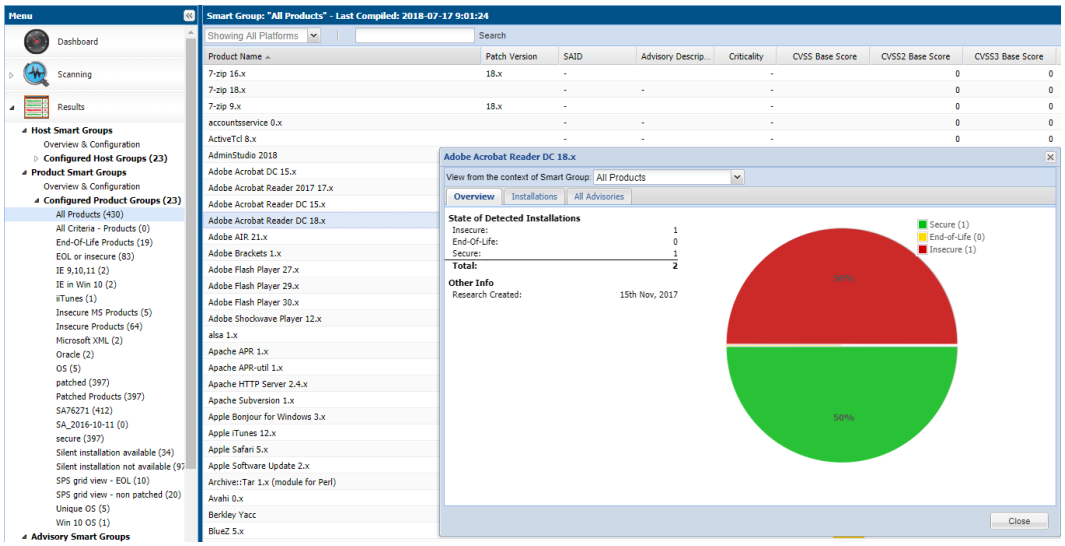


Figure -2: Flexera Package System (SPS) grouped view

The **Research Created** date was added to the **Dashboard**, **Completed Scan** and **Smart Group** views to display the date when a product has been added to Software Vulnerability Manager's vulnerability database (CSIL-8514).



Revert to last successful scan after Windows scan failure

If a Windows scan fails to complete, the patch status will revert to the last successful scan to avoid a false positive of a completed scan (CSIL-8466).

Agent now supports recovery settings

When installing the Software Vulnerability Manager 2018 Agent for Windows, Administrators can configure the agent recovery settings on a per deployment basis. The agent recovery settings are co-located in the agent package with the Run-As-User, Proxy and Site variables. For the online help reference, see Agent Configuration Options (CSIL-8101).

Agent Recovery Setting Option	Description
--service-failure-actions <actions>	Failure actions and their delay time (in milliseconds), separated by / (forward slash) – e.g., run/5000/reboot/800. Valid actions are <run|restart|reboot>. (Must be used in conjunction with the --service-failure-reset option)
--service-failure-reset <period>	Length of period of no failures (in seconds) after which to reset the failure count to 0 (may be INFINITE). (Must be used in conjunction with --service-failure-actions)
--service-failure-command <command line>	Command line to be run on failure.
--service-failure-reboot <message>	Message broadcast before rebooting on failure.
--service-failure-flag	Changes the failure actions flag setting of a service. If this setting is not specified, the Service Control Manager (SCM) enables configured failure actions on the service only if the service process terminates with the service in a state other than SERVICE_STOPPED. If this setting is specified, the SCM enables configured failure actions on the service if the service enters the SERVICE_STOPPED state with a Win32 exit code other than 0 in addition to the service process termination as above. This setting is ignored if the service does not have any failure actions configured.

Resolved Issues

Software Vulnerability Manager 2018 R4 (Cloud Edition) has resolved the following issues:

- No SAID listings for End-of-Life products
- Time-out span for patching has increased from 60 to 180 seconds
- Silent parameter and user added paths are retained for the SPS wizard
- “Patched” is now labeled “Secure”
- Whitelisting personal IP addresses
- Polish special characters now appear in installation file paths for exported CSV reports

- Dashboard option for Smart Groups has been removed
- Issue with site reporting
- Connecting to the SCCM data for import scan using TLS 1.2
- Mac OS X Agent listing of application metadata after scanning

No SAID listings for End-of-Life products

No Secunia Advisory IDs (SAID) will be listed for End-of-Life (EOL) products, as Flexera does not assign vulnerabilities to EOL products. For the online help reference, see Configured Product Smart Groups (CSIL-8520).

Time-out span for patching has increased from 60 to 180 seconds

The time-out span for patching has increased from 60 to 180 seconds. You have more time to create patching packages (SPS) for grouped packages (32/64 bit), which resolves the browser time-out issue (CSIL-8499 and CSIL-8578).

Silent parameter and user added paths are retained for the SPS wizard

The silent parameter is retained for the SPS wizard. You will no longer be prompted to install new patching packages (CSIL-8581). User added paths still appear if you select the previous screen in step 3 of the SPS wizard (CSIL-8602).

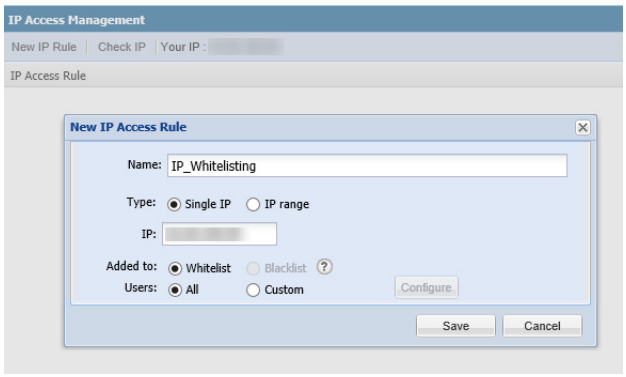
“Patched” is now labeled “Secure”

“Patched” is now labeled “Secure” in the following Software Vulnerability Manager 2018 locations (CSIL-8631):

- Dashboard
- Completed scan > Device pop-up check box
- Column headers for smart groups and patching packages
- Report configuration
- PDF reports

Whitelisting personal IP addresses

In the Administration module under **IP Access Management**, you can create an IP Access Rule for your personal IP address. For quick reference, your IP address will appear in the top row of the IP Access Management window so that it can be entered in the IP field (CSIL-8617). For the online help reference, see IP Access Management (Requires the Software Vulnerability Manager 2018 Plug-in).



Polish special characters now appear in installation file paths for exported CSV reports

Polish special characters (Examples: ą, ć, ę, ł, ń, ó, ś, ź, ż) now appear in the installation file paths column for exported Host and Products CSV reports after performing the following steps (CSIL-8663):

1. Open Excel and select the appropriate CSV report.
2. For Encoding, select UT8.
3. Save as the CSV (Comma delimited) format.

Dashboard option for Smart Groups has been removed

The Dashboard drop down option for Smart Groups has been removed from the following dashboard portlets until the historical statistical information can be correctly analyzed (CSIL-6199):

- Critically 5 Week History - Highly critical
- Critically 5 Week History - Moderately critical
- Critically 5 Week History - Less critical
- Critically 5 Week History - No critical

Issue with site reporting

Computers when connected to the active directory sometimes reported sites as "Not registered in Active Directory". This issue has been corrected. Computers connected to the active directory should report the correct site after it is scanned via the Software Vulnerability Manager Agent. Computers should belong to the active directory tree specified in the active directory settings page (CSIL-8655).

Connecting to the SCCM data for import scan using TLS 1.2

The Software Vulnerability Manager Agent has been updated to have the ability to connect with the SCCM SQL Server database over Transport Layer Security (TLS) 1.2 (CSIL-8710).

Mac OS X Agent listing of application metadata after scanning

The Mac OS X Agent has been updated to be able to read binary plist (property list) files. This new ability to scan for additional software details may result in the detection of an increased number of software titles. It is recommended that you upgrade to this improved version of our Mac OS X Agent (version 7.6.0.4) (CSIL-8775).

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 2018 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/
- 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.

Disclaimer

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. The provision of such information does not represent any commitment on the part of Flexera. Flexera makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Flexera shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The software described in this document is furnished by Flexera under a license agreement. The software may be used only in accordance with the terms of that license agreement. It is against the law to copy or use the software, except as specifically allowed in the license agreement. No part of this document may be reproduced or retransmitted in any form or by any means, whether electronically or mechanically, including, but not limited to: photocopying, recording, or information recording and retrieval systems, for any purpose other than the purchaser's personal use, without the express, prior, written permission of Flexera.