Software Vulnerability Manager 2018 R5 (Cloud Edition)

(formerly Corporate Software Inspector)

Release Notes

October 2018

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

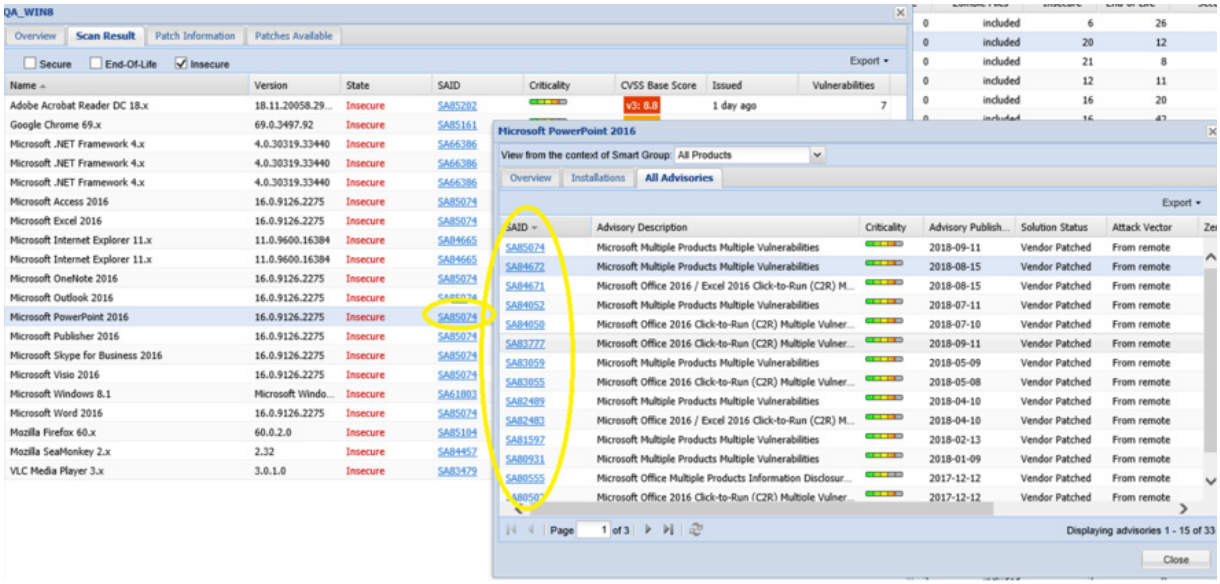
Software Vulnerability Manager 2018 R5 (Cloud Edition) includes the following new features and enhancements:

- Microsoft Office 365 detection
- Reduce agent traffic to server for better performance
- Detect missing security updates from Microsoft System Center
- Include --delete-all-settings for Mac agents
- Mac agents to use lower priority background thread

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

Microsoft Office 365 detection

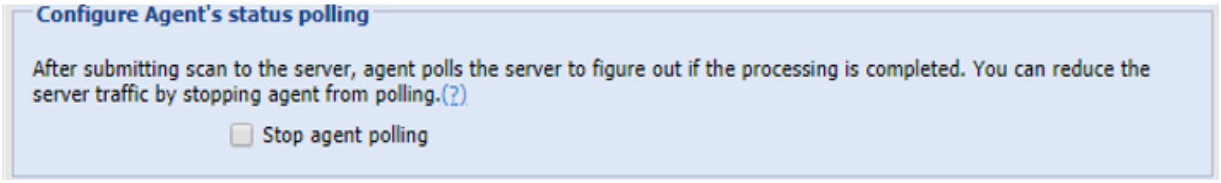
Due to a change in how Microsoft identifies Office 365 patches, we have made a new change to server logic to accommodate this scenario. As a result, you may notice additional vulnerability detections for Office 365 in this release (CSIL- 8757).



Reduce agent traffic to server for better performance

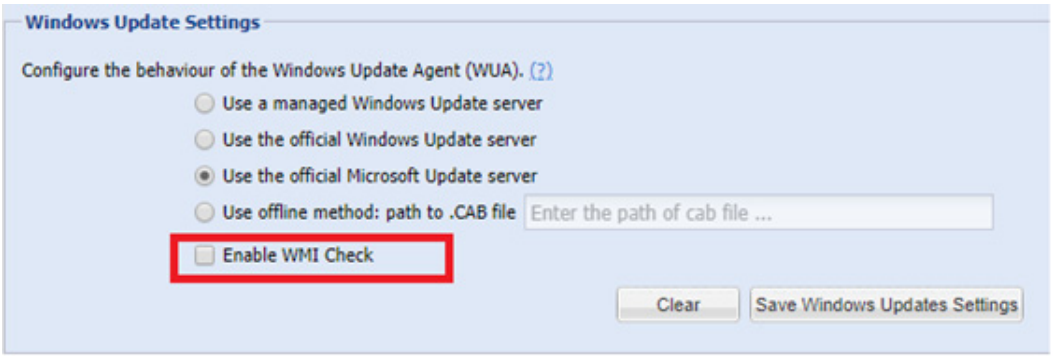
To address a server's high CPU usage during a high volume of scan data, this release includes a configuration enhancement for the agent's status pulling. Previously after uploading data to the server, the agent used to poll the server for a status of the scan process. When the server is handling a high volume, such polling translates to

higher traffic. Agent polling was intended for debugging purposes only and is not needed for core functionality. As a result, the agent polling feature has been switched off by default. You also have the ability to turn this feature ON or OFF on the settings page (CSIL-8896).



Detect missing security updates from Microsoft System Center

With this release, agents can be configured to include security updates from SCCM in the scan data. This feature can be used along with an existing missing security update collection or as the only source for missing knowledge base information (CSIL- 8777).



Include --delete-all-settings for Mac agents

The new Mac agent includes the `--delete-all-settings` parameter that will wipe out all information, including GUID, from the system to ensure it is clean to accommodate a new installation (CSIL- 8788).

Mac agents to use lower priority background thread

The new Mac agent now uses lower priority background threads to ensure minimum impact to a host's running applications (CSIL- 8794).

Resolved Issues

Software Vulnerability Manager 2018 R5 (Cloud Edition) has resolved the following issue:

- Windows 10 host now reports operating system accurately

Windows 10 host now reports operating system accurately

On the 64-bit system, Windows 10 hosts were reporting the OS name incorrectly as Enterprise Edition. This has been corrected (CSIL-8779).

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/
  - 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

Restricted Rights Legend

Disclaimer