Software Vulnerability Manager 2018 R5 (On-Premises Edition) Release Notes

October 2018

Introduction 1

New Features and Enhancements 2

- Microsoft Office 365 detection 2
- Ability to use database configured with custom ports 3
- Reduce agent traffic to server for better performance 3
- Detect missing security updates from Microsoft System Center 3
- Include --delete-all-settings for Mac agents 4
- Mac agents to use lower priority background thread 4

Resolved Issues 4

- Ensure my.cnf is not modified during upgrades 4
- Windows 10 host now reports operating system accurately 4

Product Feedback 4

System Requirements 4

Legal Information 5

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

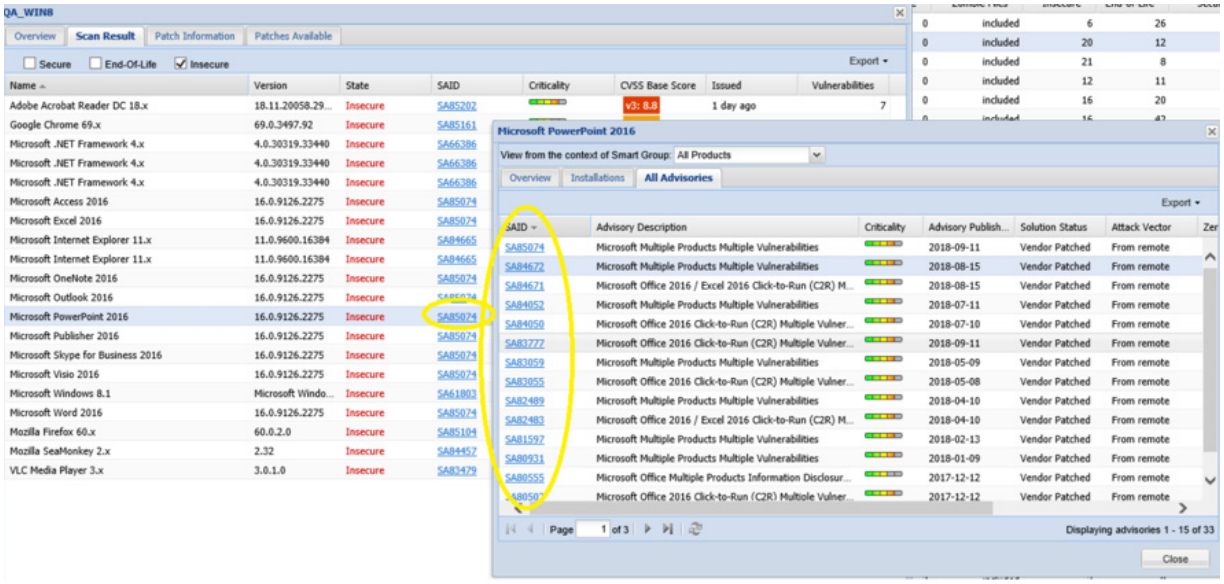
Software Vulnerability Manager 2018 R5 (On-Premises Edition) includes the following new features and enhancements:

- Microsoft Office 365 detection
- Ability to use database configured with custom ports
- 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. You may notice additional vulnerability detections for Office 365 as a result in this release (CSIL- 8757).



QA_WIN8

☐ Secure ☐ End-Of-Life ☑ Insecure

Name	Version	State	SAID	Criticality	CVSS Base Score	Issued	Vulnerabilities
Adobe Acrobat Reader DC 18.x	18.11.20058.29...	Insecure	SA85202		v3: 8.8	1 day ago	7
Google Chrome 69.x	69.0.3497.92	Insecure	SA85161				
Microsoft .NET Framework 4.x	4.0.30319.33440	Insecure	SA66386				
Microsoft .NET Framework 4.x	4.0.30319.33440	Insecure	SA66386				
Microsoft .NET Framework 4.x	4.0.30319.33440	Insecure	SA66386				
Microsoft Access 2016	16.0.9126.2275	Insecure	SA85074				
Microsoft Excel 2016	16.0.9126.2275	Insecure	SA85074				
Microsoft Internet Explorer 11.x	11.0.9600.16384	Insecure	SA84665				
Microsoft Internet Explorer 11.x	11.0.9600.16384	Insecure	SA84665				
Microsoft OneNote 2016	16.0.9126.2275	Insecure	SA85074				
Microsoft Outlook 2016	16.0.9126.2275	Insecure	SA85074				
Microsoft PowerPoint 2016	16.0.9126.2275	Insecure	SA85074				
Microsoft Publisher 2016	16.0.9126.2275	Insecure	SA85074				
Microsoft Skype for Business 2016	16.0.9126.2275	Insecure	SA85074				
Microsoft Visio 2016	16.0.9126.2275	Insecure	SA85074				
Microsoft Windows 8.1	Microsoft Windo...	Insecure	SA61803				
Microsoft Word 2016	16.0.9126.2275	Insecure	SA85074				
Mozilla Firefox 60.x	60.0.2.0	Insecure	SA85104				
Mozilla SeaMonkey 2.x	2.32	Insecure	SA84457				
VLC Media Player 3.x	3.0.1.0	Insecure	SA83479				

0	included	6	26
0	included	20	12
0	included	21	8
0	included	12	11
0	included	16	20

Microsoft PowerPoint 2016

View from the context of Smart Group: All Products

SAID	Advisory Description	Criticality	Advisory Publish...	Solution Status	Attack Vector
SA85074	Microsoft Multiple Products Multiple Vulnerabilities		2018-09-11	Vendor Patched	From remote
SA84672	Microsoft Multiple Products Multiple Vulnerabilities		2018-08-15	Vendor Patched	From remote
SA84671	Microsoft Office 2016 / Excel 2016 Click-to-Run (C2R) M...		2018-08-15	Vendor Patched	From remote
SA84052	Microsoft Multiple Products Multiple Vulnerabilities		2018-07-11	Vendor Patched	From remote
SA84050	Microsoft Office 2016 Click-to-Run (C2R) Multiple Vulner...		2018-07-10	Vendor Patched	From remote
SA83777	Microsoft Office 2016 Click-to-Run (C2R) Multiple Vulner...		2018-09-11	Vendor Patched	From remote
SA83059	Microsoft Multiple Products Multiple Vulnerabilities		2018-05-09	Vendor Patched	From remote
SA83055	Microsoft Office 2016 Click-to-Run (C2R) Multiple Vulner...		2018-05-08	Vendor Patched	From remote
SA82489	Microsoft Multiple Products Multiple Vulnerabilities		2018-04-10	Vendor Patched	From remote
SA82483	Microsoft Office 2016 / Excel 2016 Click-to-Run (C2R) M...		2018-04-10	Vendor Patched	From remote
SA81597	Microsoft Multiple Products Multiple Vulnerabilities		2018-02-13	Vendor Patched	From remote
SA80931	Microsoft Multiple Products Multiple Vulnerabilities		2018-01-09	Vendor Patched	From remote
SA80555	Microsoft Office Multiple Products Information Disclosur...		2017-12-12	Vendor Patched	From remote
SA80507	Microsoft Office 2016 Click-to-Run (C2R) Multiple Vulner...		2017-12-12	Vendor Patched	From remote

Page 1 of 3

Displaying advisories 1 - 15 of 33

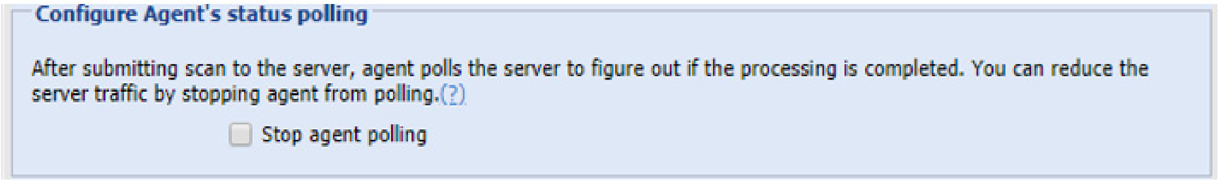
Ability to use database configured with custom ports

Software Vulnerability Manager 2018 can now work with a database installed on non-default port (CSIL-4005). This can be configured by running `installationProcess.sh` script (CSIL-8777).

Reduce agent traffic to server for better performance

To address server high CPU usage during high volume of scan data, the following enhancements have been added to this release.

- Previously after uploading data to 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, this has been switched off by default. You have the ability to turn this feature ON or OFF on the settings page (CSIL-8896).



Configure Agent's status polling

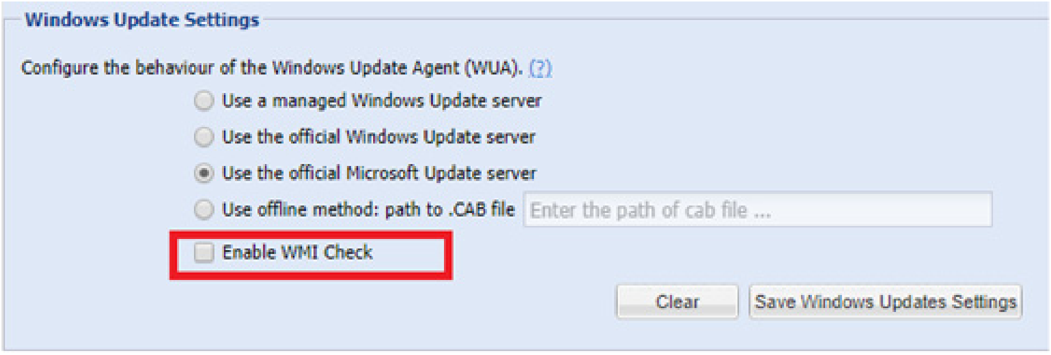
After submitting scan to the server, agent polls the server to figure out if the processing is completed. You can reduce the server traffic by stopping agent from polling.(?)

□ Stop agent polling

- New Agent code has been enhanced to include a logic to determine if the scan data being uploaded to the server is the same as the prior scan. If it is, then the agent does not upload the data to the server, thereby decreasing traffic on the server. On the server side, this logic is turned off by default and is only recommended to be turned on for situations where clients are doing daily scans, Live Update is enabled, and the host machines are relatively stable in terms of software installed on them. Server logic can be further tuned with parameter SKIP_ON_SAME_SCAN_HASH in `config.ini` which controls the number of scans after which the agent is required to send a full scan data to the server. By default, the value of this parameter is zero. Setting it to a number greater than zero will enable this feature (CSIL -8833).

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 existing missing security update collection or as only source for missing knowledge base information (CSIL- 8777).



Windows Update Settings

Configure the behaviour of the Windows Update Agent (WUA). (?)

○ Use a managed Windows Update server

○ Use the official Windows Update server

● Use the official Microsoft Update server

○ Use offline method: path to .CAB file Enter the path of cab file ...

□ Enable WMI Check

Include --delete-all-settings for Mac agents

The new Mac agent include has `--delete-all-settings` parameter that will wipe out all information including GUID from the system to ensure its clean to accommodate new installation (CSIL- 8788).

Mac agents to use lower priority background thread

New mac agent will now use lower priority background threads to ensure minimum impact to a host's running applications (CSIL- 8794).

Resolved Issues

Software Vulnerability Manager 2018 R5 (On-Premises Edition) has resolved the following issues:

- Ensure my.cnf is not modified during upgrades
- Windows 10 host now reports operating system accurately

Ensure my.cnf is not modified during upgrades

Installation process has been modified to verify if user wants to modify my.cnf file during upgrades (CSIL-8771).

Windows 10 host now reports operating system accurately

On 64-bit system, Windows 10 hosts were reporting 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 `http(s)://csi_server_name/`.
- The `http(s)://csi_server_name/` should be white-listed in the Firewall/Proxy configuration

- First-Party cookie settings at least to Prompt (in Internet Explorer)
- Allow session cookies
- A PDF reader

Legal Information

Copyright Notice

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/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