

# Software Vulnerability Manager 2018 R5 (Cloud Edition)

(formerly Corporate Software Inspector)

## Release Notes

October 2018

<b>Introduction</b> .....	<b>1</b>
<b>New Features and Enhancements</b> .....	<b>2</b>
Microsoft Office 365 detection .....	2
Reduce agent traffic to server for better performance .....	2
Detect missing security updates from Microsoft System Center .....	3
Include --delete-all-settings for Mac agents .....	3
Mac agents to use lower priority background thread .....	3
<b>Resolved Issues</b> .....	<b>3</b>
Windows 10 host now reports operating system accurately .....	4
<b>Product Feedback</b> .....	<b>4</b>
<b>System Requirements</b> .....	<b>4</b>
<b>Legal Information</b> .....	<b>4</b>

## 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).

Name	Version	State	SAID	Criticality	CVSS Base Score	Issued	Vulnerabilities
Adobe Acrobat Reader DC 18.x	18.11.20058.29	Insecure	SA85202	High	v3: 8.8	1 day ago	7
Google Chrome 69.x	69.0.3497.92	Insecure	SA85161	High			
Microsoft .NET Framework 4.x	4.0.30319.33440	Insecure	SA66386	High			
Microsoft .NET Framework 4.x	4.0.30319.33440	Insecure	SA66386	High			
Microsoft .NET Framework 4.x	4.0.30319.33440	Insecure	SA66386	High			
Microsoft Access 2016	16.0.9126.2275	Insecure	SA85074	High			
Microsoft Excel 2016	16.0.9126.2275	Insecure	SA85074	High			
Microsoft Internet Explorer 11.x	11.0.9600.16384	Insecure	SA84665	High			
Microsoft Internet Explorer 11.x	11.0.9600.16384	Insecure	SA84665	High			
Microsoft OneNote 2016	16.0.9126.2275	Insecure	SA85074	High			
Microsoft Outlook 2016	16.0.9126.2275	Insecure	SA85074	High			
Microsoft PowerPoint 2016	16.0.9126.2275	Insecure	SA85074	High			
Microsoft Publisher 2016	16.0.9126.2275	Insecure	SA85074	High			
Microsoft Skype for Business 2016	16.0.9126.2275	Insecure	SA85074	High			
Microsoft Visio 2016	16.0.9126.2275	Insecure	SA85074	High			
Microsoft Windows 8.1	Microsoft Windo...	Insecure	SA61803	High			
Microsoft Word 2016	16.0.9126.2275	Insecure	SA85074	High			
Mozilla Firefox 60.x	60.0.2.0	Insecure	SA85104	High			
Mozilla SeaMonkey 2.x	2.32	Insecure	SA84457	High			
VLC Media Player 3.x	3.0.1.0	Insecure	SA82479	High			

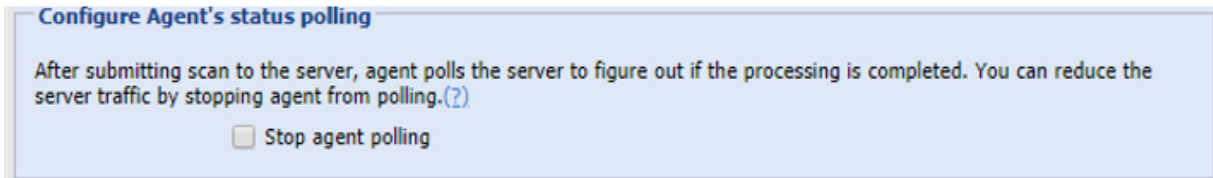
  

SAID	Advisory Description	Criticality	Advisory Publish...	Solution Status	Attack Vector
SA85074	Microsoft Multiple Products Multiple Vulnerabilities	High	2018-09-11	Vendor Patched	From remote
SA84672	Microsoft Multiple Products Multiple Vulnerabilities	High	2018-08-15	Vendor Patched	From remote
SA84671	Microsoft Office 2016 / Excel 2016 Click-to-Run (C2R) M...	High	2018-08-15	Vendor Patched	From remote
SA84052	Microsoft Multiple Products Multiple Vulnerabilities	High	2018-07-11	Vendor Patched	From remote
SA84050	Microsoft Office 2016 Click-to-Run (C2R) Multiple Vulner...	High	2018-07-10	Vendor Patched	From remote
SA83777	Microsoft Office 2016 Click-to-Run (C2R) Multiple Vulner...	High	2018-09-11	Vendor Patched	From remote
SA83059	Microsoft Multiple Products Multiple Vulnerabilities	High	2018-05-09	Vendor Patched	From remote
SA83055	Microsoft Office 2016 Click-to-Run (C2R) Multiple Vulner...	High	2018-05-08	Vendor Patched	From remote
SA82489	Microsoft Multiple Products Multiple Vulnerabilities	High	2018-04-10	Vendor Patched	From remote
SA82483	Microsoft Office 2016 / Excel 2016 Click-to-Run (C2R) M...	High	2018-04-10	Vendor Patched	From remote
SA81597	Microsoft Multiple Products Multiple Vulnerabilities	High	2018-02-13	Vendor Patched	From remote
SA80931	Microsoft Multiple Products Multiple Vulnerabilities	High	2018-01-09	Vendor Patched	From remote
SA80555	Microsoft Office Multiple Products Information Disclosur...	High	2017-12-12	Vendor Patched	From remote
SA80500	Microsoft Office 2016 Click-to-Run (C2R) Multiple Vulner...	High	2017-12-12	Vendor Patched	From remote

## Reduce agent traffic to server for better performance

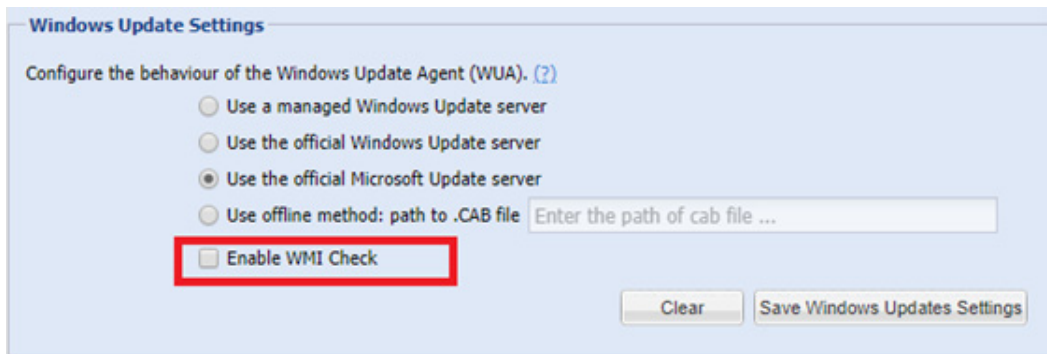
To address a server's high CPU usage during a high volume of scan data, this release includes a configuration enhancement for the agent's status pulling. Previously after uploading data to the server, the agent used to poll the server for a status of the scan process. When the server is handling a high 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](http://crl.verisign.net)
  - [crl.thawte.com](http://crl.thawte.com)
  - <http://crl3.digicert.com>
  - <http://crl4.digicert.com>
  - [http://\\*.ws.symantec.com](http://*.ws.symantec.com)
  - [https://\\*.secunia.com/](https://*.secunia.com/)
  - [http://\\*.symcb.com](http://*.symcb.com)
  - [http://\\*.symcd.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

Copyright © 2018 Flexera.

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 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.