Software Vulnerability Manager 2018 R4 (On-Premises Edition)

(formerly Corporate Software Inspector)

Release Notes

August 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 R4 (On-Premises Edition) includes the following new features and enhancements:

- MySQL 5.7.22 support in RHEL 7

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

MySQL 5.7.22 support in RHEL 7

Software Vulnerability Manager 2018 now supports MySQL server 5.7+/Mariadb 10.x for its database on RHEL 7. Upgrading to this release involves modification to schema that requires the availability of enough free temp space on the database server. It is recommended to have at least 1.5 times the file size of the biggest `csi_device_software.frm` file in the database data directory (inside the Software Vulnerability Manager private database directory) (CSIL-8694).

Resolved Issues

Software Vulnerability Manager 2018 R4 (On-Premises Edition) has resolved the following issues:

- 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

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 7.6.1.4) (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 `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

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.