FLEXERA
SOFTWARE™

FLEXERA SOFTWARE®
Corporate Software Inspector

Corporate Software Inspector Cloud Edition
Release Notes

March 2016-May 2017

Introduction

Flexera's Corporate Software Inspector is a Vulnerability and Patch Management Software Solution that completes and targets the 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 Corporate Software Inspector, IT Operations and Security Teams are empowered to take control of the Vulnerability Threat from both Microsoft and non-Microsoft (third-party) product vulnerabilities, covering Microsoft Windows, Mac OSX, and Red Hat Enterprise Linux.

Corporate Software Inspector scanning technology takes a different approach than other vulnerability scanning solutions by conducting non-intrusive scans to accurately identify all installed products and plugins on the system.

Corporate Software Inspector integrates seamlessly with Microsoft® WSUS and System Center Configuration Manager.

Release History

The following table summarizes the Corporate Software Inspector Cloud Edition Release History from March 2016 through May 2017.

Release Date (Day.Month.Year)	Release Number	Release Details
03.05.2017	CSI 2016 R6	**Resolved Issues:** ● CSIL-6361: User-entered site name / group name during installation of a single host agent is now seen in the **Scanning Via Local Agents** console. ● CSIL-8070: Editing an existing published patching package no longer adds a random path on the third step of creating a Software Package System (SPS). ● CSIL-8142: Users can now create custom patching packages for Adobe products with multiple language options. ● CSIL-8144: Can now advance to step 3 of the package configuration wizard ● CSIL-8149: Adobe Shockwave update now shows up on hosts that need it ● CSIL-8156: MAC agent site parameter -g now works
20.02.2017	CSI 2016 R4 Cloud / On-Premises HotFix	**Resolved Issues:** CSIL-8069: CSI plugin is able to connect, during collection import plugin (comsurogate) consumes 100% of memory and makes system freeze/crash

Release Date (Day.Month.Year)	Release Number	Release Details
01.02.2017	CSI 2016 R4 (7.5.0.6)	**Features:** • CSIL-7998: Windows components rated Insecure after applying updates • CSIL-8009: SA73206 - Red Hat Kernel version is no longer rated Insecure by CSI agent (RHEL agent) • CSIL-8053: Added hash_key to columns for database console export of csi_device_software_binding & csi_device_software **Resolved Issues:** • CSIL-7988: Resolved multiple Personal Software Inspector integration issues with Corporate Software Inspector • CSIL-7989: AD integration now works for Partitions. • CSIL-8032: Decrypt vuln_title in the table csi_device_software in the on-premise version • CSIL-8042: Linux machines with security issues marked as patched • CSIL-8045: Instant access now works for partitions that need live updates, and there are zero-day advisories listed in the last hour of the vulntrak.vuln table • CSIL-8074: Upgraded the Personal Software Inspector version to install with Corporate Software Inspector

Release Date (Day.Month.Year)	Release Number	Release Details
08.12.2016	CSI 2016 R3 (7.5.0.3)	**Resolved Issues:** • CSIL-8038: VA PHP Error parsing /etc/csi/config.common.ini • CSIL-8036: PDF Reports are now generated on the 7.5.1.3-0 RPMs • CSIL-8035: Database backup issue was resolved when upgrading from 7.4.1.x to 7.5.1.3-0 on RH7 w/ MySQL 5.7 • CSIL-8023: RHEL agents now install/remove service via command line switches • CSIL-8021: MAC agent check-in shows Windows platform • CSIL-8016: Implemented a separate process for Corporate Software Inspector Cloud releases • CSIL-8015: Multi-language packs are now functioning for Firefox • CSIL-8014: [JN Data] CSI 7 on RHEL 7 does accept foreign characters in OU names, CSI Agent fails Scan • CSIL-7991: SCCM collections are now visible after 1606 upgrade • CSIL-7986: Mac OS X is no longer reported as Windows • CSIL-7985: When exporting "Installations" from a Windows product, missing KBs are now included in export • CSIL-7983: CSI root admin profile; how do I mark the checkbox "Allow User to see Completed Scans and Agents" • CSIL-7982: Escalated: MAC agent issue • CSIL-7264: Daemon 7.2.0.10 installation shows password in error Msg • CSIL-7130: CSI root admin profile; how do I mark the checkbox "Allow User to see Completed Scans and Agents"? • CSC-164: Daemon 7.2.0.10 installation shows password in output file
27.10.2016	CSI 2016 R2 SP1 HotFix (7.4.0.2)	**Resolved Issues:** • Support for SCCM 1606 • Unencrypted Vulnerability titles in csi_device_software exports • Agent installation fix (upgrade works again)

Release Date (Day.Month.Year)	Release Number	Release Details
28.09.2016	CSI 2016 R2 SP1 (7.4)	**Features:** • CSC-299: "Activate collect network information" was updated in the User Guide • CSC-277: Documented in the User Guide that the Daemon service needs to disconnect from SC-CM DB before SC-CM upgrade • CSI-7870: The Zombie files setting is now a global setting and is only changeable by the partition admin • Checkbox for SCCM Collection Name to Sitename is now available in the Cloud • CSI-7859 CSI no longer finds files in the recycle bin **Resolved Issues:** • CSC-345: Initial CSV report configuration creates PDF report and saves the settings as a PDF • CSC-324: Can now advance to step 3 of the package configuration wizard • CSC-246: Long running SCCM import now works • CSC-216: Zombie Files are now being omitted after selecting to hide them • CSC-215: Microsoft Updates are no longer showing up after deselecting it in the settings • CSC-107: CSI Activity Log only shows activity of the user logged in. • CSI-7149: Binaries now clean up old installations (Daemon, Agent, Browser Plugin, SC-Plugin • CSC-326: Browser Plugin installs into C:\ when installed with /S • CSI-7847: Same site name when importing multiple collections

Release Date (Day.Month.Year)	Release Number	Release Details
03.08.2016	CSI 2016 R2 (7.3.0.3) Hotfix	**Resolved Issues:** ● New Daemon binary with fix for SCCM Connection sharing ● CSI-7818: Package error "SHA1 checksum for ... does not exist" has been resolved ● CSI-7808: Cab file Monitoring no longer generates too many log messages ● CSI-7838: SC Collection as Site Name now works ● CSI-7839: SC Collection as Site Name checkbox now saving in the SCCM Plugin. The checkbox value now resets after doing an SCCM import. ● CSI-6747: LIMIT 1 replication warnings are now generated when an agent checks in ● CSI-7835: Grouped SPS packages are now targeting the correct max versions ● CSI-7848: Corrected the copyright notice on login page ("2015" -> "2015 - 2016") ● CSC-109: Smart Group Notifications overview, Smart Group Monitored is displaying Notification name. ● CSC-147: Count information is now in Host Smartgroups. ● CSC-71: Export page always exports all products/hosts for Smart Groups. ● CSC-296: Dashboard elements now show Smart Group names in report. ● CSC-311: When creating a Smart Group which displays System Score < 100% machines with 100% were displayed (rounding issue). ● CSC-187: CSI Reports, email recipients now appear if you change the page to select multiple recipients. ● CSC-310: Now able to export Dashboard view.

Release Date (Day.Month.Year)	Release Number	Release Details
24.06.2016	CSI 2016 R2 (7.3)	**Enhancements** ● Group SPS packages by solution in CSI and SCCM **Resolved Issues:** ● Changes to the View settings in the SPS packages page are now persistent. ● CSI-7155 (CSC-156): SCCM inventory import now picks up the OS version. ● CSI-7139 (CSC-138): Changing Language files in STEP2 (SPS wizard) no longer generates an error in regards to SHA1 checksum. ● The SPS system is now capable of distinguishing between already published 82x and 64x packages (only for packages created with the Corporate Software Inspector 2016 R2 or later).
26.04.2016	CSI 2016 (7.2) Hotfix	● The CSI can now export very large data sets into CSV files. PDF exports have also been improved, but very large PDFs still cause problems. ● The performance of SCCM Imports has been improved significantly. In some cases imports will take less than 50% of the time they took before the improvements. ● Fixed the too-frequent session timeout for the Corporate Software Inspector Internet Explorer Plug-In and SCCM Plug-In.
20.04.2016	CSI 2016 (7.2) Hotfix	● CSC-146: A fix for where advisories being wrongly displayed for patched products. ● CSC-148: A fix for where no new custom scan rules could be created. ● DEVOPS-1940: A fix which should solve an issue where some customers could not recompile their smart groups. ● We increased the session timeout from one hour to two hours.
07.04.2016	CSI 2016 (7.2.0.6) Hotfix	● Fixed the Browser Plug-In to import SCCM collections from SCCM 2007 ● Fixed the Daemon to import SCCM collections from SCCM 2007

Release Date (Day.Month.Year)	Release Number	Release Details
31.03.2016	CSI 2016 (7.2) Hotfix	• CSC-108: Corrected numbering for the insecure count in the SPS view • CSC-125: Packages created with versions < CSI 2016 (7.2) are now marked as already created • CSC-112: Sorting in Smart Groups now works on all columns
17.03.2016	CSI 2016 (7.2) Hosted	**Integration:** • Flexera rebranding **Features:** • SONY Reporting • Warnings in SPS • Microsoft external signing • SCCM Collection import **Resolved Issues:** • Performance • Numbers in dashboard

System Requirements

To use the Corporate Software Inspector console, your system should meet the following requirements:

- Minimum resolution: 1024x768

- 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 addresses crl.verisign.net, crl.thawte.com, http://*.ws.symantec.com and https://*.secunia.com/ 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

Copyright © 2017 Flexera. All Rights Reserved.

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 www.flexerasoftware.com/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.