Corporate Software Inspector 2018 R1 (On-Premises Edition) Release Notes

March 2018

Introduction 1

New Features and Enhancements 2

- Display all advisories affecting a product 2
- Additional updates to Patch Template feature 3
- Enhanced installation script for Corporate Software Inspector 3
- Prevent excessive polling for status by agent 3
- Integrated online help for Corporate Software Inspector 3

Resolved Issues 3

- Detection of Microsoft products in host with language packs 4
- Using “not in” criteria when viewing or editing Smart Group criteria for Operating System 4
- Fixed SCCM plug-in import for Microsoft KBs 4
- Renamed Zero-Day Advisory Filters 4
- Available page shows only 25 packages when more packages are available 5
- Updated Online Help section: Install the Mac Agent 5
- Missing EOL products for Last Week’s Data on Dashboard 5

System Requirements 5

Legal Information 5

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.

New Features and Enhancements

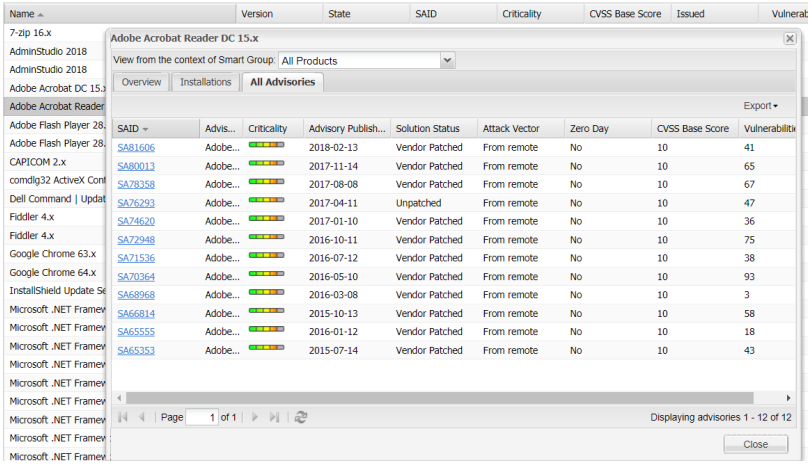
Corporate Software Inspector 2018 R1 (On-Premises Edition) includes the following new features and enhancements:

- Display all advisories affecting a product
- Additional updates to Patch Template feature
- Enhanced installation script for Corporate Software Inspector
- Prevent excessive polling for status by agent
- Integrated online help for Corporate Software Inspector

Note • *To see the following new features and enhancements in your Corporate Software Inspector interface, you must refresh the cache in your browser. You can use the shortcut key CTRL+R.*

Display all advisories affecting a product

A new Advisory tab has been added to the detailed pop-up screens. This tab lists all current and past advisories that affect a product. Note that these listed advisories could be related to different platforms (CSIL-8381).



Additional updates to Patch Template feature

New cron job will run on the server that will continuously monitor newly available patches and update the patch URL for all existing patch templates as required. It will also invalidate patch templates that are no longer valid.

When a Patch Template is opened, its path will update automatically based on the latest assessment data available (CSIL-8444).

Enhanced installation script for Corporate Software Inspector

If the SQL user does not have the proper grant permissions, the Corporate Software Inspector installation will abort, and the following error message will appear: "`Aborting installation - User root does not have GRANT permission.`" (CSIL-8433)

Prevent excessive polling for status by agent

To prevent the Corporate Software Inspector Agent from flooding the server with requests for scan status every second, new polling logic has been implemented. This new polling logic helps increase the scalability of the web server to support more agents (CSIL-8506).

Integrated online help for Corporate Software Inspector

After logging on to Corporate Software Inspector, users can press F1 to connect to the relevant online help page (CSIL-8469).

Resolved Issues

Corporate Software Inspector 2018 R1 (On-Premises Edition) has resolved the following issues:

- Detection of Microsoft products in host with language packs
- Using "not in" criteria when viewing or editing Smart Group criteria for Operating System
- Fixed SCCM plug-in import for Microsoft KBs
- Renamed Zero-Day Advisory Filters
- Available Packages page now displays dynamically the list of available packages
- Updated Online Help section: Install the Mac Agent
- Missing EOL products for Last Week's Data on Dashboard

Detection of Microsoft products in host with language packs

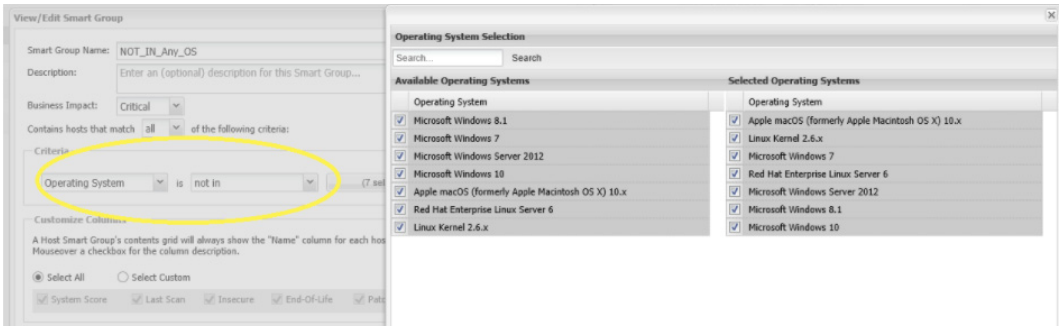
Corporate Software Inspector was not detecting a few Microsoft products like IIS when they scanned hosts with language packs and were installed in their default windows system directory. This was because on such machines the window api reported filenames with an `.exe.mui` extension instead of just `.exe`. This issue has been fixed (CSIL-8210).

Note • *This fix might lead to the detection of more Microsoft products, and users might see an increase in the installed counts on their Corporate Software Inspector Dashboard.*

Using “not in” criteria when viewing or editing Smart Group criteria for Operating System

The issue of incorrect host counts when using the “Operating System -> not in” criteria for Host smart groups has been fixed.

Note • *For Linux platforms, “Linux Kernel” and “Red Hat Enterprise Linux Server” are both considered operating systems. To obtain accurate smart group host counts, you only need to select one of the Linux operating systems (CSIL-8458).*



Fixed SCCM plug-in import for Microsoft KBs

Fixed issues related to SCCM plug-in not reporting Microsoft KBs (CSIL-8498).

Renamed Zero-Day Advisory Filters

Under **Results > Advisory Smart Groups > Overview and Configuration** the Zero-Day Advisory filters:

- “Currently Affecting You” was renamed “Advisories that Affected You”
- “Historic List of Zero-Day Advisories” was renamed “All Advisories”

For further details, see http://helpnet.flexerasoftware.com/csionprem/Default.htm#helplibrary/Overview_and_Configuration_2.htm (CSIL-8484).

Available page shows only 25 packages when more packages are available

WSUS/System Center was incorrectly reporting the number of available packages. This issue has been fixed (CSIL-8454).

Updated Online Help section: Install the Mac Agent

Previously, documentation suggested giving higher privileges to `csia.exe` than required. It is highly recommended that this be changed by executing command "`chmod +x csia`". This change will prevent "`csia`" from having more privileges than it needs.

The updated help section can be found here: http://helpnet.flexerasoftware.com/csionprem/Default.htm#helplibrary/Install_the_Mac_Agent.htm (CSIL-8545).

Missing EOL products for Last Week's Data on Dashboard

EOL product without vulnerability IDs were shown for the current day's data, but they were not shown in last week's data. This issue has been corrected (CSIL-8396).

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 `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

Restricted Rights Legend

Disclaimer