Corporate Software Inspector 2016 R10 (Cloud Edition)
Release Notes

December 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.

New Features and Enhancements

Corporate Software Inspector 2016 R10 (Cloud Edition) includes the following new features and enhancements:

- **Patch Template for easier deployment to WSUS**
- **Added Operating System criteria to Product Smart Groups**
- **Corporate Software Inspector Agent upgraded to Transport Layer Security (TLS) 1.2**

**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.

**Patch Template for easier deployment to WSUS**

Users can now save a template of their patches via the Patch Template feature for a product. With the Patch Template feature, the user can prepopulate Flexera’s Software Package System (SPS) four-step deployment process and publish directly to WSUS using previously selected options (CSIL-8398).

**Added Operating System criteria to Product Smart Groups**

Operating System criteria has been added as a new filter for Product Smart Groups to report results as two separate lists: client products and server products (CSIL-6870).

**Corporate Software Inspector Agent upgraded to Transport Layer Security (TLS) 1.2**

To implement a more secure communication protocol, the Corporate Software Inspector Agent now only supports TLS 1.2. Corporate Software Inspector no longer supports TLS 1.0 and TLS 1.1 (CSIL-8399).
Resolved Issues

Corporate Software Inspector 2016 R10 (Cloud Edition) has resolved the following issues:

- Network appliance agent can be removed from the Corporate Software Inspector console.
- Sudden spike in discovered applications for Corporate Software Inspector Cloud Edition

Network appliance agent can be removed from the Corporate Software Inspector console.

The network appliance agent can now be removed from the Corporate Software Inspector console (CSIL-8140).

Sudden spike in discovered applications for Corporate Software Inspector Cloud Edition

We fixed a bug related to the Weekly dashboard where weekly data was reporting only unique product and ignoring installation counts. This bug showed up as a sudden spike in installation counts when the current day’s data was compared with week old data. To implement the fix, a new column has been added to the table csi_device_software_history. For the Corporate Software Inspector Cloud Edition, we are rolling out this change incrementally to prevent disruption. We expect a complete roll out to all active customers within a week of this release (CSIL-8395).

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.