# Corporate Software Inspector 2016 R10 (On-Premises 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 (On-Premises Edition) includes the following new features and enhancements:

- New Operating System criteria for Product Smart Groups
- Corporate Software Inspector Agent upgraded to Transport Layer Security (TLS) 1.2
- Corporate Software Inspector Agent can accept token and site details via command line
- Removed zero count installations path from Flexera's Software Package System (SPS) wizard

***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.*

## New Operating System criteria for Product Smart Groups

Operating System criteria has been added as a new filter for Product Smart Groups (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).

## Corporate Software Inspector Agent can accept token and site details via command line

Agents for the server edition now support passing the agent token and other relevant details via command line or registry. When agents are downloaded from the UI, token, userid, and server details are embedded into the agent executable. This process creates an issue when trying to deploy agents across very large enterprises when hosts are spread across multiple partitions. To resolve this issue, a copy of the agent from the web server can be deployed, and configuration details can be kept in a Windows registry or specified as a command line parameter to the agent. The agent configuration parameters can be obtained via email from the agent download page in the website (CSIL-8405).

## Removed zero count installations path from Flexera's Software Package System (SPS) wizard

In Step 3 of the SPS installation, paths with zero counts are included by default. These paths represent scan data from hosts that are no longer active. Going forward, such zero count paths will not be included. Users will have to explicitly include them in the package (CSIL-8420).

# Resolved Issues

Corporate Software Inspector 2016 R10 (On-Premises Edition) has resolved the following issues:

- Upgrade RPM package in Linux to enable Zero Day Vulnerability module
- Network appliance agent can be removed from the Corporate Software Inspector console.
- Software configuration enhancements
- Validation rules established for saving Patch Template Names
- Agent uninstalls older versions of agent when installed as a service

## Upgrade RPM package in Linux to enable Zero Day Vulnerability module

Older versions, when upgraded to the latest rpm build, were not including the Zero Day Vulnerability module. This issue has been fixed. After upgrading the RPM package, the Zero Day Advisories listing should appear under **Results** (CSIL-8017).

## 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).

## Software configuration enhancements

New installations of CSI will configure website to use TLS 1.2 protocol for SSL connections. TLS 1.0 and TLS 1.1 are considered insecure by the industry, so they will be disabled by default. The Following settings have been added to `/etc/httpd/conf.d/secunia-csi-httpd.conf file` (CSIL-8342).

```
“SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1”

"SSLHonorCipherOrder On"

"SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH:!aNULL:!MD5:!RC4:!DES "
```

## Agent uninstalls older versions of agent when installed as a service

When installed as a service, older versions of the agent were not uninstalled. This issue has been fixed (CSIL-8447).

# 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

## 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.