FLEXERA
SOFTWARE

FLEXERA SOFTWARE®
Corporate Software Inspector

Corporate Software Inspector 2016 R7 (Cloud Edition)
Release Notes

July 2017

Introduction

Flexera Software 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

Corporate Software Inspector 2016 R7 (Cloud Edition) includes the following new features:

- Filter Host Smart Groups on Missing Microsoft Knowledge Base (KB) Articles

- Site Name Search under Single Host Agents

- Listing of Affected Installations for Advisory Smart Groupss

- Notification to Customers when Password Recovery Settings are not Configured

Filter Host Smart Groups on Missing Microsoft Knowledge Base (KB) Articles

One option for filtering Host Smart Group information is by Microsoft KB articles to create a report of hosts that are missing one or several specific KB articles. This filtering can be used for new or existing Host Smart Groups (CSIL-8204).
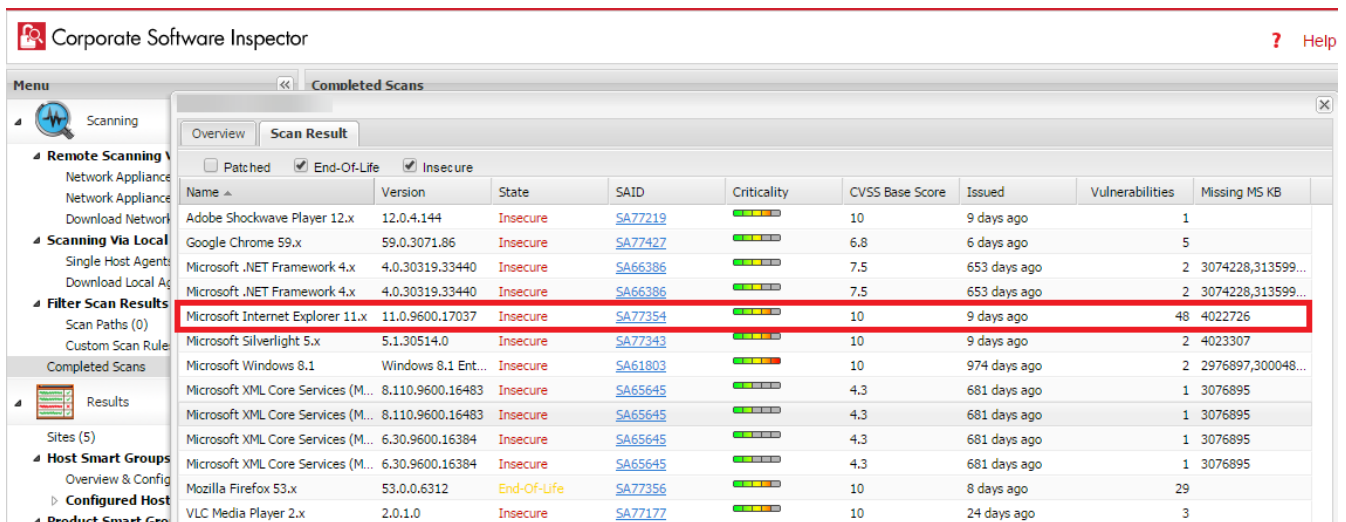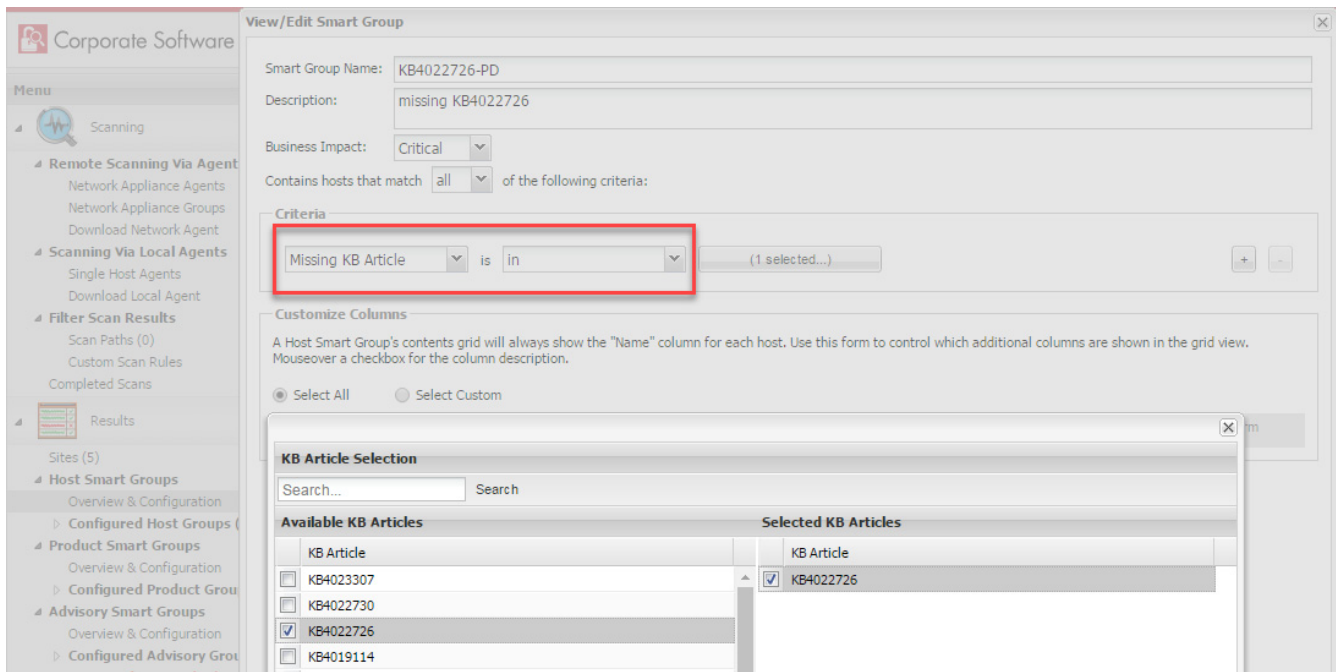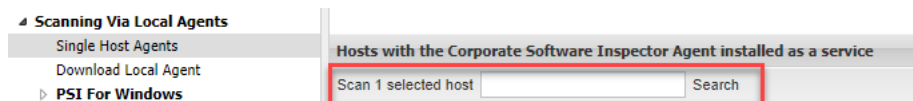
Site Name Search under Single Host Agents

Corporate Software Inspector 2016 R7 now allows you to search for a site name to edit the configuration for agents joined to different sites (CSIL-8129) using the following procedure.

Task   *To search for a site name to edit the configuration for agents joined to different sites:*

1. Navigate to the **Single Host Agents** view.

2. In the **Scan 1 selected host search box**, enter the sitename and host name using the "OR" condition to show the respective result.

Listing of Affected Installations for Advisory Smart Groups

The Advisory Smart Group module now has a listing of All Advisories Under the **Configured Advisory Group** view. For each advisory, you can click the corresponding number listed in the **Installations**, **Products**, and **Hosts** columns. After clicking the number in the **Installations** column, you will see a list of affected installations per host (CSIL-6871).

? Help   Logout

Smart Group: "All Advisories" - Last Compiled: 2017-07-17 14:37:35

Export ▾

SAID	Advisory Description ▲	Criticality	Zero-Day	Advisory Published	Vulnerabil…	Solution Status	CVSS…	Attack Vector	Impact	Installations	Products	Hosts
SA76208	Adobe Acrobat / Reader XI Desktop Multiple Vulnerabili…		No	11th Apr, 2017	47	Vendor Patched	10	From Remote	System Access, E:	8	2	
SA70400	Adobe Flash Player / AIR Multiple Code Execution Vuln…		Yes	10th May, 2016	30	Vendor Patched	10	From Remote	System Access	1	1	
SA									System Access	5	2	
SA									System Access, E:	6	2	
SA									System Access	7	2	
SA									System Access	1	1	
SA									Security Bypass, (	2	1	
SA									Privilege Escalatic	4	1	
SA									undefined, Securi	1	1	
SA									System Access	1	1	
SA									Security Bypass	5	3	
SA									System Access	10	3	
SA									Denial of Service,	6	1	
SA									System Access, E:	6	1	
SA									Security Bypass, !	3	2	
SA									Exposure of Sensi	4	2	
SA									Security Bypass, (	1	1	
SA									System Access, E	1	1	
SA									System Access, E:	2	2	
SA									System Access, D	1	1	
SA									Exposure of Sensi	1	1	
SA									ecurity Bypass, I	1	1	
SA									stem Access	1	1	
SA									stem Access	1	1	
SA									ecurity Bypass, I	1	1	
SA									stem Access	6	3	
SA									ndefined, Spoofi	1	1	
SA									ndefined, Spoofi	27	2	
SA									stem Access, D	10	4	
SA7									oofing, System	1	1	
SA6									stem Access	3	1	
SA7									ivilege Escalatic	1	1	

SA76208 Affected Installations

Export ▾

Product	Version ▲	Host
Adobe Reader X 10.x	10.1.0.534	Win7TestPc
Adobe Reader X 10.x	10.1.4.38	PSCCM
Adobe Reader XI 11.x	11.0.19.15	sushma_win81A
Adobe Reader XI 11.x	11.0.19.15	sushma_win81B
Adobe Reader XI 11.x	11.0.19.15	SBABA_WIN81
Adobe Reader XI 11.x	11.0.19.15	AMOHAN-WIN8-…
Adobe Reader XI 11.x	11.0.19.15	AMOHAN-W10-16
Adobe Reader XI 11.x	11.0.19.15	BLR-P7109660

SA76208 Affected Products

Export ▾

Product ▾
Adobe Reader XI 11.x
Adobe Reader X 10.x

SA76208 Affected Hosts

Export ▾

Host ▾

Notification to Customers when Password Recovery Settings are not Configured

If you have not configured your Corporate Software Inspector password recovery settings and you need to reset your password at login, you can restore access to your user account. After clicking Forgot your password? Flexera Software will send an email to the email address used at the time of your account creation. The email subject line will state: "Flexera Software Corporate Software Inspector Password Recovery Failed". The email will state: "Dear customer, You have not configured the password recovery settings. Please contact your admin/Support." (CSIL-8051)

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

Resolved Issues

Corporate Software Inspector 2016 R7 (Cloud Edition) has resolved the following issues:

- Corporate Software Inspector Agents do not obtain the agent configuration and display empty values for check-in and scanning intervals

- Advisory Smart Group does not display 2017 data for "Advisory Published is Exactly" criteria

Corporate Software Inspector Agents do not obtain the agent configuration and display empty values for check-in and scanning intervals

To address this issue, further clarification has been provided in the user guide for selecting options under **Edit Site Configuration** for Single Host Agents (CSIL-8193).

Important • *When selecting options under* **Edit Site Configuration**, *note that:*

- Any edits to the scan schedule will come into affect only after the currently scheduled scan has completed. Each agent could potentially have a scan scheduled at different times. Therefore, any new scan configuration edit will affect the scan schedule at various times.

- Any edits made to the **Agent Check-In Frequency** option or selecting the **Schedule Next Scan** option **Scan host as soon as possible** will come into effect only after an agent has checked in as per the previously set scan frequency.

- The scan configuration settings set on the Corporate Software Inspector website are not automatically transmitted to the agents. The agents have to connect to the Corporate Software Inspector website as per their prior scheduled **Agent Check-In Frequency** before the agents become aware of the new scan configuration edits.

Advisory Smart Group does not display 2017 data for "Advisory Published is Exactly" criteria

To address this issue, the following View/Edit Smart Group Configuration statement was added to the user guide (CSIL-8198).

For each Advisory Smart Group, you can create or edit the advisory criteria using the Zero-Day Status and Advisory Published criteria. Both criteria include dates, which are created using the Coordinated Universal Time (UTC). Therefore, the local zone date of the user could be different from the zone the advisory data was saved in, which may lead to a difference in advisory lists.

Legal Information

Copyright Notice

Intellectual Property

For a list of trademarks and patents that are owned by Flexera Software, see www.flexerasoftware.com/intellectual-property. All other brand and product names mentioned in Flexera Software products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

Disclaimer