Cisco Services Platform Collector 2.7.4.7

Features and Resolved Defects

June 2019

Contents

Table of Contents

1. Introduction

This document provides information about what's new in the Common Services Platform Collector (CSPC) 2.7.4.7. This release fixes key security vulnerabilities along with the new features and an upgrade patch that would benefit all the customers.

The CSPC software provides an extensive collection mechanism to collect various aspects of customer network information. CSPC connects to the discovered devices providing delivery of network information to network administrators and network engineers. Data collected by CSPC is used by several Cisco Advanced and Technical Service offers to provide detailed reports and analytics for both the hardware and software, such as inventory reports, product alerts, configuration best practices, network audits and so on.

2. Features

Following features are added in this release to enhance security and to overcome the operational issue.

- CSPC now interprets IP address, Hostname and Domain Name entries in the seedfile to perform hostname resolution by eliminating the need for local DNS lookup. In addition, auto discovery has been made optional in "Seedfile Management" so that users can schedule it as per their convenience.
- This release supports Cisco Unified Communications Manager (CUCM) and Unity Collection for collaboration assessments. Additional collaboration applications will be supported in the subsequent releases.
- "Show devices" CLI has been enhanced to allow users to search based on the hostnames
- Customizations in the settings of CSPC such as discovery, inventory, application or connectivity settings are retained when the collector is upgraded to the next version.
- New specific Device Access Verification (DAV) error messages in CSPC helps in better analysis for the DAV failed devices and further troubleshooting.
- If the collection fails for the device, then the TimeInventoryUptime and TimeConfigUpdated fields will be empty for those devices in the ElementInventoryInfo file instead of keeping the old time stamps.
- After upgrade to new available version, you can view the changes made to custom Data Sets, Platform Rules, Integrity Rules, Collection Profile, Masking Rules, and Custom DSIRT Rules.
- Health uploads are limited to the latest 10K lines. This avoids the health uploads growing too large and impacting available disk space.
- Option added in the Network Optimization Service (NOS) configurer installation to schedule health, DAV, and inventory jobs immediately or later.
- Seedfile management and interpretation changes for smarter and reliable discovery.
- Custom regex patterns are added in the settings for the syslogs and also creates the separate syslog files for parsed and unparsed syslogs.
- Inventory summary reports include config not applicable device count along with config collected and config failed device count.
- Syslog upload is based on the standard calendar specifying the date and time range not the CSPC received timestamp.
- All logging messages indicate the module name with the currently logged message contents. Also separate log files are provided for installation logs and console logs.
- Flexibility to select the list of the protocol and set the order to try the protocols for DAV. Try all options is provided to try all of the selected protocols for DAV.

- REST API supports pushing the seed file from a customer system to CSPC.
- Multi Service Collection Profile clubs one or more Collection Profiles from different services and internally consolidates the datasets for collection.
- Option to delete the appliance certificate from collector as required.
- Support for Prime Infrastructure 3.1 with RI Addon Pull model for seed file sync.
- Improved version of Upgrade Tab on CSPC UI with changes, such as New icon, auto status refresh, and displays all the installed updates
- . CSPC to forwarding all the raw syslog (up to 20 million) to CRA that is, OnPrem tool that provides real time remediation. Also to enable CSPC for cloud ray to get device details and working credentials from CSPC API.
- Flexibility to the user to read and upload syslog's based on CSPC received time rather than device time stamp. This option can be used for the collectors that are managing the devices across different time zones and different countries.
- Notifying with the appropriate error message in notification on CSPC home page and as well as in upload logs in case of upload failure due to certificate invalidity.
- Readiness and Enhancement on the CSPC VSEM data file to support NPNG. Also to populate additional information in the VSEM file that provides more granular details about the devices and its status.
- Exporting the DAV details from the CSPC UI and consistency between the CLI and UI reports for DAV results.
- CSPC supports collection for video product devices mainly for http/https datasets. The devices includes TP, Endpoints, VCS/Expressway, and all video products those are SNMP enabled.
- CSPC collects specific OID's to get the health information and upload the information via health uploads for external platform components such as CIMC, ESXi, and pfSense/CSR v1000 that supports SNMP.
- Enhancing the syslog upload by providing an option to the end user to select the parsed and unparsed syslogs based on the need during the upload that eases the further analysis of huge syslog messages.
- Certifying the show commands through Rest API for connected TAC's Diagnostic Bridge which schedules the periodic execution of show commands.
- Capability of CSPC to provide the FQDN (Sysname) as part of device list XML API
- Infrastructure to support Diagnostic Bridge (Prime Infrastructure) capability of CSPC to provide domain name as a part of device list XML API
- Enhance the CSPC installation UI Wizard to select the "Time Field" in a drop-down to select the time format with 0 to 23 hours and 0 to 59 minutes.
- Support for transactional customers where CSPC is not installed in customer premise. To install CSPC on the VM and also on user laptop. CSPC functionality should be supported.
- Reduce the disc space usage by the CSPC files by compressing the file sizes to allow the more efficient usage of the collector resources
- Allow users to access adminshell when CSPC is not up and running
- Provide support for IPv6 for collector Management by providing support to manage and access the Collector using IPv6 address
- Moving from three versions of OVAs (Small/Med/Large) to one configurable OVA with Ultra Small/Small/Medium/large configurations and OVA to be available for minor (x.x and x.x.x) releases of CSPC as well
- LCM Manager provides the list of available upgrades to the LCM agent on the Install base collector appliances. In turn LCM agent on the install base collector appliance connects to IDA to download the latest updates. The IDA shall redirect the request to the repository. IDA is now getting decommissioned. and is replaced by ASD.

- A pop up notification to alert the user that a new version is available when the version being used is EOL and not supported.
- Build an inventory of all the files and data (settings, configurations, and so on) to be backed up. Also provides ability to backup and restore the backed up data
- Include required diagnostic Packages in RPM
- GRUB password must conform to InfoSec standard. Without it, anyone can get into GRUB and login to single user mode and shutdown or change password
- Make JeOS patch common so it can be installed on NCCM box also, remove references to CSPC_HOME and also have admin shell scripts for Maria DB.
- Support of the latest version of CSPC for OnPrem 2.0
- CSPC needs to have an image that can install CSPC 2.7 base and its components: adminshell/LCM, Connectivity, and CSPC 2.7. Separate Installation for adminshell/LCM and Connectivity are required for older appliances that do not have these installed, but user can upgrade.
- Connectivity and Software upgrade requires system to be in same date and time (connectivity HGWY and CSPC have to be on same time). The only way currently to achieve this is for customers to open a support case and configure it via CLI. Provide interface to modify settings via RMC (various timeouts, upload proxy, and collection profiles)
- Use of Google Tink crypto library for encryption and for rotation of the data encryption key to provide greater safety for customer data. In the next release, further extensions will be done to allow customers to deposit the keys in Cloud based Key Management Services (AWS and Google Cloud).
- One Time Password (OTP) scheme is implemented to enable easy and quicker way to rest admin password. This was one of the major concern expressed by many self-service customers and partners. Without this feature, the only option if customer forgets the admin password is to reinstall the CSPC.
- CSPC users can now opt-out from some of the stringent security login features such as Captcha, frequent mandatory password changes and frequent logouts in case of short inactivity. This is expected to improve the customer experience as it was one of the most talked topics on the support communities.
- Supports CLI data collection and several icurl command collection using HTTP from NX9K Application Centric Infrastructure (ACI).
- “View Access Verification Results” report is enhanced to show the IP address details of each device in order to enable further troubleshooting in case of access verification issues.
- Show primary entitled CSP registration ID in the home page of CSPC along with collector name to help customers, partners and support engineers to uniquely identify the collector quickly.
- Addressed ~40 STIG compliancy related findings.
- Ability to collect “show tech” command from XML editor in CSPC and ability to view the collected command output in its entirety.
- Multi-level authorization has been put in place for Remote Management Console for accessing terminals and collector report data. This will help to tighten the access to collector reports and terminals on RMC

To upgrade existing CSPC to latest version refer to CSPC Upgrade Guide

3. Resolved Defects

Below are the resolved defects in CSPC 2.7.4.7

Bug ID	Description
CSCuy79296	Issue in typing “3” character on AdminShell Commands
CSCvb03809	Job Upload Status is displaying incorrect success message on failed uploads
CSCvb77184	System is sending old records in CollectionErrors
CSCvb86639	Collection Profile based VSEM conversion has conversion time in ElementInventoryInfo.download
CSCvb93504	CASP patches cannot be installed on existing CSPC with older adminshell
CSCvd10471	Not all devices in PI are being extracted to CSPC devices are getting extracted partially
CSCvd44549	LMS password with special characters not accepting on RI-Addon
CSCvd82321	Time is displayed in UTC timezone even when server timezone is correct.
CSCvd93403	Audit Response file not getting generated.
CSCve02935	Root login should not have Lockout Enforced in Pam_Tally2
CSCve19094	DAV results incorrect(false negatives and incorrect negative)
CSCve39388	Results in DAV report is misleading for audit collection.
CSCve41070	Config Data not downloading
CSCve80418	DAV is failing while going through jump server to collect the configurations
CSCve89060	Nexus 9k devices with `SysObjID` “1.3.6.1.4.1.9.12.3.1.3.1626” not getting selected via CSPC UI
CSCvf02260	`job_schedule_discovery_runnow.sh` CLI has a issue with `_enableloopback flag`
CSCvf48042	CSPC UI software updates error
CSCvf49086	SNMP V3 collection took long time for collection
CSCvf52993	Adminshell connection refused if no network connection is available
CSCvg42884	Collection Profile Scheduler disrupted after 2.7.2 Upgrade
CSCve95059	NPE when in tunnel reconnects
CSCve99947	CSPC Remote Tunnel Not Staying Established - WebSocket Read EOF
CSCvf61035	Increased Global Timeout causing delay in total collection time. (Customer: CTS)
CSCvf65189	TEG does not reconnect because of error in handling EOFException
CSCvf75195	Show version is not collecting for csp2100 device
CSCvf75227	RP4.2: CSP device is not classified properly
CSCvf75374	Not able to get Bidirectional URL, even if Web socket is enabled
CSCvf82261	SFTP backup/restore failing
CSCvf82630	Collection Profiles does not stop even after audit duration

Bug ID	Description
CSCvf86697	Websocket disabled after few days
CSCvf90401	ApplyIPSSignature failing with error message
CSCvg04197	SNMP String collected by show snmp command which is not masked
CSCvg29635	ElementInventory.download populated with null values for TIMECONFIGUPDATED and TIMEINVENTORYUPTIME
CSCui33836	Validation not happening for IP and arguement
CSCuz81805	Failed to login devices, if enable password not configured.
CSCvc49466	Unable to schedule the Audit from CSPC GUI due to the time sync issue.
CSCvd36933	SNTC OVA - Images ask admin password to be reset twice with first login (Ref - CSCuu73657)
CSCve04671	CSPC 2.7: User Login Attempt Lockout settings need to be relaxed
CSCve56315	Issues in creating Dynamic group based on IP in 2.7
CSCve71097	CNA skips devices with different hostname and primary device name for devices chosen in CSPC
CSCve89284	“Advanced Option” in DAV Module throws error from CSPC GUI
CSCvf15853	Data extraction fails as soon as starting with HPNA 10.x[Seedfile option not enabled]
CSCvf20550	CSPC Wizard: Fails to execute update for (DNS/Proxy/Hostname/NTP/Timezone/Timestamp)
CSCvf36446	CSPC: Delete CSPC Entitlement Fails
CSCvf48042	CSPC GUI software updates error
CSCvf49121	Incomplete SNMP collection for CRS devices with CSPC
CSCvf50079	CSPC FTP pfSense version 2.3.2 and FTP is no longer supported
CSCvf57533	Discovery job description not getting reflected in Discovery jobs list
CSCvf61035	Increased Global Timeout causing delay in total collection time.
CSCvf72490	Export syslog shows wrong details
CSCvf73811	IP range discovery moving unreachable devices to “Unmanaged” state
CSCvf75402	CSPC is not able to connect to WLC device after to push config via ssh
CSCvf82630	CPs does not stop even after audit duration
CSCvf85675	Seedfile import issue
CSCvf92875	Non Managed devices affect CSPC performance
CSCvg15976	Issues with sort by column in 2.7.1
CSCvg20473	Unable to switch user to root CSPC 2.2.2 base OVA image
CSCvg29635	ElementInventory.download populated with null values for TIMECONFIGUPDATED and TIMEINVENTORYUPTIME
CSCvg35076	DAV : “Run discovery before DAV” option not working properly (device skipped)
CSCvg42884	Collection Profile Scheduler disrupted after 2.7.2 Upgrade
CSCvg57638	CSPC 2.7.2: dav.xml on transport file is malformed

Bug ID	Description
CSCvh50640	Audit collection got stuck and never stops.
CSCvh93443	CSPC Diagnostic Bridge Integration - Extra Char Present in Collected CLI Configs
CSCve06613	Smart sleep functionality during CSPC installation
CSCve98438	CSPC deleting all devices in a group even if filter applied
CSCvg41666	Dataset filter in collection data viewer not working properly
CSCvg44802	Registration Portal: CSPC NOS cert generated with lower case customerID
CSCvg54690	CSPC duplicate detection should be VRF-aware
CSCvg70613	Job run status export option not working
CSCvh07543	SNTC: CSPC collector versions not reflecting updates
CSCvh12895	Audit issue - Prompt collection does not run when the audit is scheduled
CSCvh44113	CSPC GUI: Software upgrades are becoming stuck with status “Apply-In-Progress”
CSCvh51393	CSPC 2.7.1 detects device to be the duplicate of an unmanaged IP address
CSCvh60290	CSPC - TEG is not registered after upgrades, which is causing uploads to fail
CSCvh78442	CSPC is not parsing syslogs properly when multiple source files are present.
CSCvh79086	CSPC CLI upgrade getting stuck with message “Apply-in-progress”
CSCvh93443	CSPC Diagnostic Bridge Integration - Extra Character Present in Collected CLI Configs
CSCvi31931	LCM not using DNS for hostname resolution
CSCvi34865	Incorrect specification char encoding format
CSCvi50779	CSPC not picking exact credentials
CSCvi90560	Auto update job triggered but apply did not triggered after download
CSCvj82821	SysDescription was missing in the virtually added devices because of this HTTP dav was failing
CSCvk06098	Connected bridge was not able to process the response XML data due to non-printable characters in the XML file.
CSCvk07572	VSEM data was not getting created in Network_1.xml file for specific use case, where the duplicate device state is inconsistent.
CSCvk22119	Reporting portal was not able to process the DAV.xml data due to non-printable characters in the xml file.

Security Bugs

Below are the Security bugs in CSPC 2.7.4.7

BugID	Description
CSCvh84427	Nessus: CentOS 6 : kernel (CESA-2018:0169)
CSCvh47854	Nessus Security: Meltdown and Spectre - kernel update CVE-2017-5753, CVE-2017-5715, CVE-2017-5754
CSCvh49631	High security vulnerability found on CSPC kernel CVE CVE-2017-5715, CVE CVE-2017-5753, CVE CVE-2017-5754

BugID	Description
CSCvj13310, CSCvj13304	JAVA-SE Upgrade to 8u172 or latest
CSCvj52723	Apache Tomcat 7.0.x < 7.0.82 / 8.5.x < 8.5.23 Multiple Vulnerabilities:
CSCvj58152	Kernel (CESA-2018:1319) and kernel (CESA-2018:1651) (Spectre)
CSCvj84604	CentOS 6 - props needs to be updated
CSCvj52723	Apache Tomcat 7.0.x < 7.0.82 / 8.5.x < 8.5.23 Multiple Vulnerabilities:
CSCvk42896	Nessus: gnupg2 (CESA-2018:2180) package requires to be updated
CSCvk42911	Nessus: kernel (CESA-2018:2164) (Spectre) Kernel package requires to be updated
CSCvk53684	Nessus - CentOS 6 : ding-libs / sssd (CESA-2018:1877)
CSCvk65814	Oracle Java SE Multiple Vulnerabilities (July 2018 CPU) (Unix)
CSCvk73519	Apache Tomcat 8.5.0 < 8.5.32 Multiple Vulnerabilities
CSCvm00332	yum-utils (CESA-2018:2284) requires to be updated
CSCvm99444	Multiple vulnerabilities reported in Oracle Java and this lets remote users gain elevated privileges, remote and local users access to modify data, and remote users deny service. CVEs: CVE-2018-3136, CVE-2018-3139, CVE-2018-3149, CVE-2018-3150, CVE-2018-3157, CVE-2018-3169, CVE-2018-3180, CVE-2018-3183, CVE-2018-3209, CVE-2018-3211, CVE-2018-3214, CVE-2018-13785 Java version (1.8.0_192) is updated to the latest to resolve the above CVEs
CSCvm43387	Vulnerability in bind package (CESA-2018:2571) This flaw may allow a remote attacker to launch a denial of service attack on the system. CVEs: CVE-2018-5740 Bind package version upgrade to bind-utils-9.8.2-0.68.rc1.el6_10.1 to resolve the above CVEs.
CSCvm59990	Kernel upgrade to resolve FragmentSmack And CESA-2018:2846 vulnerabilities. CVEs: CVE-2018-5391 This updates the kernel version of CentOS 6 to the latest (2.6.32-754.6.3.el6.x86_64) that resolves FragmentSmack vulnerability and the CVEs mentioned above.
CSCvm99360	Vulnerability in nss package (CESA-2018:2898) CVE-2018-12384 nss pacakage updated to the latest version that resolve the vulnerability and the above CVE
CSCvm17314	access_verifier.download file was not creating during upload when there are duplicate devices with inconsistent state in CSPC Handled the inconsistent state devices during the upload functionality
CSCvm91664	Out of memory issue was coming when multiple syslog files with huge size mounted on the CSPC. Changed the Queue limit for processing the syslogs

4. Available Resources

Additional information regarding installing and configuring the collector are covered in below documents:

- CSPC Quick Start Guide
- CSPC Upgrade Guide
- CSPC Installation Guide
- CSPC User Guide
- Troubleshooting Guide

Software Download

- CSPC Image Download Center

5. Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA 6/3/2019