

# Cisco Services Platform Collector CSPC 2.10.0.7

Release Notes  
June 2023  
(Updated March 2024)



## Table of Contents

<b>1. Introduction</b> .....	<b>3</b>
CSPC Supported Browsers.....	3
<b>2. What's New</b> .....	<b>3</b>
<b>3. Defects Addressed</b> .....	<b>4</b>
<b>4. Enhancements</b> .....	<b>4</b>
<b>5. Known Issues</b> .....	<b>4</b>
<b>6. Available Resources</b> .....	<b>5</b>
Software Download.....	5
<b>7. Legal Information</b> .....	<b>5</b>

## 1. Introduction

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 TechnicalService 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.

### CSPC Supported Browsers

- Internet Explorer 9 to 21
- Mozilla Firefox 27 to 109
- Google Chrome 57 to 120

## 2. What's New

This section provides information about what's new in the Common Services Platform Collector (CSPC) 2.10.0.7

- Key security vulnerability fixes that would benefit all customers.
- Customer found defects were resolved.
- Rules Package 4.19
- Support for TLS 1.3

### 3. Defects Addressed

Following are the defects addressed as part of CSPC 2.10.0.7

Identifier	Title
CSCwf20608	Oracle Java SE Multiple Vulnerabilities (April 2023 CPU)
CSCwe96842	CentOS 7 : zlib (CESA-2023:1095) The remote CentOS Linux host is missing a security update
CSCwe96863	CentOS 7 : nss (CESA-2023:1332)The remote CentOS Linux host is missing a security update
CSCwe96867	CentOS 7 : kernel (CESA-2023:1091) The remote CentOS Linux host is missing a security update
CSCwe96870	CentOS 7 : openssl (CESA-2023:1335) CESA-2023:1335 Important CentOS 7 openssl Security Update
CSCwe96877	CentOS 7 : samba (CESA-2023:1090) The remote CentOS Linux host is missing a security update
CSCvv66322	CSPC vulnerable to 'Java JMX RMI Accessible with Common Credentials (Unauthenticated check)'
CSCwf32516	IOS-XE device fail to recognize User EXEC mode prompt after login
CSCwe13184	Range base Discover method not working with multiple SNMP version
CSCwc80500	CSPC discovery ICMP status in DAV report in the original list
CSCwd80530	Fix DAV status/message for post-login use-cases (Other than authentication failed false positive)

### 4. Enhancements

- BSVBE-12983 – SHA upgrade
- RP 4.19 upgrade
- Support for TLS 1.3

### 5. Known Issues

CSCwe95589 LCM upgrade is not working.

## 6. Available Resources

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

- [CSPC Quick Start Guide](#)
- [CSPC Installation Guide](#)
- [CSPC User Guide](#)
- [Troubleshooting Guide](#)

### Software Download

- [CSPC Image Download Center](#)

## 7. 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](http://www.cisco.com/go/offices).

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

June 2023  
Updated March 2024