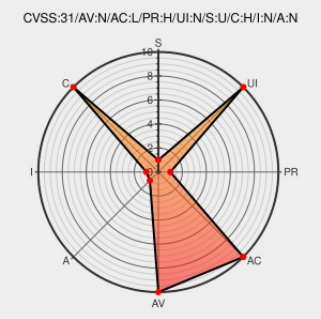
CVE-2021-40130

Published on: 11/18/2021 12:00:00 AM UTC

Last Modified on: 08/05/2022 11:50:00 AM UTC

CVE-2021-40130 - advisory for cisco-sa-CSPC-ILR-8qmW8y8X

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Common Services Platform Collector from Cisco contain the following vulnerability:

A vulnerability in the web application of Cisco Common Services Platform Collector (CSPC) could allow an authenticated, remote attacker to specify non-log files as sources for syslog reporting. This vulnerability is due to improper restriction of the syslog configuration. An attacker could exploit this vulnerability by configuring non-log files as sources for syslog reporting through the web application. A successful exploit could allow the attacker to read non-log files on the CSPC.

CVE-2021-40130 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Affected Vendor/Software: **Cisco** - **Cisco Common Services Platform Collector Software** version **n/a**

CVSS3 Score: 4.9 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Cisco Common Services Platform Collector Improper Logging Restriction Vulnerability	tools.cisco.com text/html	CISCO 20211117 Cisco Common Services Platform Collector Improper Logging Restriction Vulnerability

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Common Services Platform Collector	All	All	All	All

cpe:2.3:a:cisco:common_services_platform_collector:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@SystemTek_UK	Cisco Common Services Platform Collector Improper Logging Restriction Vulnerability [CVE-2021-40130] systemtek.co.uk/2021/11/cisco-…	2021-11-18 08:49:04
@6townstechteam	Cisco Common Services Platform Collector Improper Logging Restriction Vulnerability [CVE-2021-40130] systemtek.co.uk/2021/11/cisco-…	2021-11-18 08:49:05
@CVEreport	CVE-2021-40130 : A vulnerability in the web application of Cisco Common Services Platform Collector CSPC could… twitter.com/i/web/status/1…	2021-11-18 23:58:17

← Previous ID Next ID→

CVE.report and Source URL Uptime Status status.cve.report