



CVE-2022-20669

Published on: Not Yet Published

Last Modified on: 06/03/2022 06:34:00 PM UTC

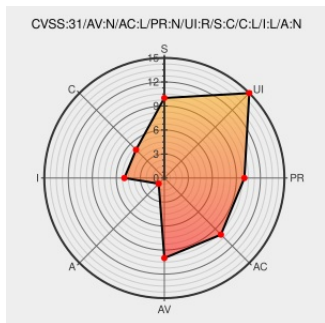
CVE-2022-20669 - advisory for cisco-sa-cspc-multi-xss-tyDFjhw

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Common Services Platform Collector](#) from [Cisco](#) contain the following vulnerability:

Multiple vulnerabilities in the web-based management interface of Cisco Common Services Platform Collector (CSPC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by

the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.

CVE-2022-20669 has been assigned by [cisco 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 - Cisco Common Services Platform Collector Software** version n/a

CVSS3 Score: **6.1 - MEDIUM**

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|----------------|------------------------|---------------------|---------------------|
| NETWORK | LOW | NONE | REQUIRED |
| Scope | Confidentiality Impact | Integrity Impact | Availability Impact |
| CHANGED | LOW | LOW | NONE |

CVSS2 Score: **4.3 - MEDIUM**

| Access Vector | Access Complexity | Authentication |
|------------------------|-------------------|---------------------|
| NETWORK | MEDIUM | NONE |
| Confidentiality Impact | Integrity Impact | Availability Impact |
| | | |

NONE

PARTIAL

NONE

CVE References

| Description | Tags | Link |
|--------------------------------|--|--|
| No Description Provided | tools.cisco.com text/html | CISCO 20220518 Cisco Common Services Platform Collector Cross-Site Scripting Vulnerabilities |

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 |
| <code>cpe:2.3:a:cisco:common_services_platform_collector:*****:*****:</code> | | | | | | |

No vendor comments have been submitted for this CVE

Social Mentions

| Source | Title | Posted (UTC) |
|--|--|------------------------|
|  @mimura1133 | Cisco RV340 VPN Router (CVE 的には Cisco Small Business RV Series) の CVE-2022-20669 の PoC と解説。 CVSS の値が高いというのがありますけど... twitter.com/i/web/status/1... | 2022-02-12 14:54:19 |
|  @CVEreport | CVE-2022-20669 : Multiple vulnerabilities in the web-based management interface of Cisco Common Services Platform... twitter.com/i/web/status/1... | 2022-05-27 14:15:36 |
|  /r/netcve | CVE-2022-20669 | 2022-05-27 15:38:34 |

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)