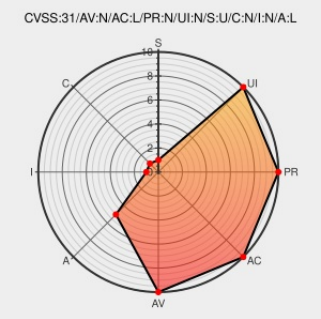
CVE-2022-20750

Published on: Not Yet Published

Last Modified on: 02/28/2022 05:49:47 PM UTC

CVE-2022-20750 - advisory for cisco-sa-rcm-tcp-dos-2Wh8XjAQ

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



Certain versions of Redundancy Configuration Manager from Cisco contain the following vulnerability:

A vulnerability in the checkpoint manager implementation of Cisco Redundancy Configuration Manager (RCM) for Cisco StarOS Software could allow an unauthenticated, remote attacker to cause the checkpoint manager process to restart upon receipt of malformed TCP data. This vulnerability is due to improper input validation of an ingress TCP packet. An attacker could exploit this vulnerability by sending crafted TCP data to the affected application. A successful exploit could allow the attacker to cause a denial of service (DoS) condition due to the checkpoint manager process restarting.

CVE-2022-20750 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as HIGH 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 Redundancy Configuration Manager** version **n/a**

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
No Description Provided	Vendor Advisory tools.cisco.com text/html	CISCO 20220216 Cisco Redundancy Configuration Manager for Cisco StarOS Software TCP Denial of Service 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	Redundancy Configuration Manager	All	All	All	All

cpe:2.3:a:cisco:redundancy_configuration_manager:*:*:*:*:*:staros:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-20750 : A vulnerability in the checkpoint manager implementation of Cisco Redundancy Configuration Manager… twitter.com/i/web/status/1…	2022-02-28 18:42:08

← Previous ID

Next ID→