

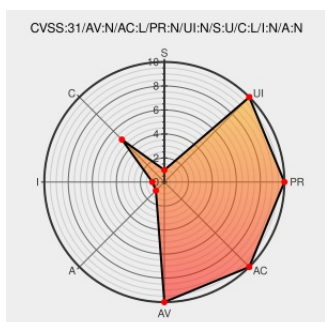


CVE-2022-29538

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:21:00 PM UTC

CVE-2022-29538

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Gemini-net](#) from [Resi](#) contain the following vulnerability:

RESI Gemini-Net Web 4.2 is affected by Improper Access Control in authorization logic. An unauthenticated user is able to access some critical resources.

CVE-2022-29538 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
GEMINI-NET™ - NETWORK & SERVICE MONITORING - RESI Informatica	www.resi.it text/html	www.resi.it/prodotti-soluzioni-commerciali/gemini-network-service-monitoring
Gruppo TIM Vulnerability Research & Advisor	www.gruppotim.it text/html	www.gruppotim.it/it/footer/red-team.html

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	Resi	Gemini-net	4.2	All	All	All
cpe:2.3:a:resi:gemini-net:4.2:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @threatmeter	CVE-2022-29538 RESI Gemini-Net Web 4.2 is affected by Improper Access Control in authorization logic. An unauthenti... twitter.com/i/web/status/1...	2022-05-12 23:01:55
 @threatmeter	CVE-2022-29538 RESI Gemini-Net Web 4.2 is affected by Improper Access Control in authorization logic. An unauthenti... twitter.com/i/web/status/1...	2022-05-13 07:09:51

[← Previous ID](#)

[Next ID →](#)