



CVE-2022-29540

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-29540
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-02 14:15:00 UTC
Updated	2022-06-09 20:11:00 UTC
Description	resi-calltrace in RESI Gemini-Net 4.2 is affected by Multiple XSS issues. Unauthenticated remote attackers can inject arbitrary HTML and JavaScript into the application. This vulnerability is caused by the lack of output encoding in the calltrace function. The vulnerability is present in the calltrace function of the RESI Gemini-Net 4.2 application. The calltrace function is used to log the execution of the application. It takes a string as input and outputs a log entry. The log entry is then displayed on the application's interface. The vulnerability is caused by the lack of output encoding in the calltrace function. The calltrace function does not escape the input string, which allows an attacker to inject arbitrary HTML and JavaScript into the application. This can be used to steal sensitive information or to perform other malicious actions.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Resi	Gemini-net	4.2	All	All	All

References

Reference	Source	Link	Tags
GEMINI-NET ™ - NETWORK & SERVICE MONITORING - RESI Informatica	MISC	www.resi.it	
www.gruppotim.it/it/footer/red-team.html	MISC	www.gruppotim.it	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

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