



CVE-2023-49694

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-49694
State	PUBLISHED
Assigner	Unknown
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-29 23:15:00 UTC
Updated	2023-12-05 01:54:00 UTC
Description	Description unavailable.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netgear	Prosafe Network Management System	All	All	All	All

References

Reference	Source	Link
Security Advisory for Vertical Privilege Escalation on the NMS300, PSV-2023-0127 - NETGEAR Support		kb.netgear.com
NETGEAR ProSAFE Network Management System (NMS300) Multiple Vulnerabilities - Research Advisory Tenable®		www.tenable.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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