



CVE-2023-1327

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

Summary

CVE	CVE-2023-1327
State	PUBLIC
Assigner	vulnreport@tenable.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-14 22:15:00 UTC
Updated	2023-03-21 17:59:00 UTC
Description	Netgear RAX30 (AX2400), prior to version 1.0.6.74, was affected by an authentication bypass vulnerability, allowing an una

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Rax30	-	All	All	All
Operating System	Netgear	Rax30 Firmware	All	All	All	All

References

Reference	Source	Link
Sign in · Cloudflare Access	MISC	drupal9.tena
Netgear RAX30 (AX2400), prior to version 1.0.6.74, was... · CVE-2023-1327 · GitHub Advisory Database · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.or
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.

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](#).

Free CVE JSON API cve.report/api

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