



CVE-2022-44194

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

Summary

CVE	CVE-2022-44194
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-22 14:15:00 UTC
Updated	2022-11-23 18:51:00 UTC
Description	Netgear R7000P V1.3.0.8 is vulnerable to Buffer Overflow via parameters apmode_dns1_pri and apmode_dns1_sec.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	R7000p	-	All	All	All
Operating System	Netgear	R7000p Firmware	1.3.0.8	All	All	All

References

Reference	Source	Link	Tags
Router login	MISC	routerlogin.net	
NETGEAR: Advanced WiFi & Networking	MISC	netgear.com	
IoT_vuln/Netgear/R7000P/11 at main · RobinWang825/IoT_vuln · GitHub	MISC	github.com	
www.netgear.com/about/security	MISC	www.netgear.com	
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.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)