



CVE-2022-30079

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

Summary

CVE	CVE-2022-30079
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-08 12:15:00 UTC
Updated	2023-08-08 14:21:00 UTC
Description	Command injection vulnerability was discovered in Netgear R6200 v2 firmware through R6200v2-V1.0.3.12 via binary /sbin

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Neatgear	R6200	r6200v2-v1.0.3.12	All	All	All
Hardware	Netgear	R6200	v2	All	All	All
Operating System	Netgear	R6200	r6200v2-v1.0.3.12	All	All	All

References

Reference	Source	Link	Tags
vulnerabilities/CVE-2022-30079.md at main · 10TG/vulnerabilities · GitHub	MISC	github.com	
r6200v2.com	MISC	r6200v2.com	
NETGEAR: Advanced WiFi & Networking	MISC	netgear.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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)