



CVE-2022-48176

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

Summary

CVE	CVE-2022-48176
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-31 00:15:00 UTC
Updated	2023-02-08 02:02:00 UTC
Description	Netgear routers R7000P before v1.3.3.154, R6900P before v1.3.3.154, R7960P before v1.4.4.94, and R8000P before v1.4.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Mr60	-	All	All	All
Operating System	Netgear	Mr60 Firmware	All	All	All	All
Hardware	Netgear	Ms60	-	All	All	All
Operating System	Netgear	Ms60 Firmware	All	All	All	All
Hardware	Netgear	R6900p	-	All	All	All
Operating System	Netgear	R6900p Firmware	All	All	All	All
Hardware	Netgear	R7000p	-	All	All	All
Operating System	Netgear	R7000p Firmware	All	All	All	All
Hardware	Netgear	R7960p	-	All	All	All
Operating System	Netgear	R7960p Firmware	All	All	All	All
Hardware	Netgear	R8000p	-	All	All	All
Operating System	Netgear	R8000p Firmware	All	All	All	All

References

Reference

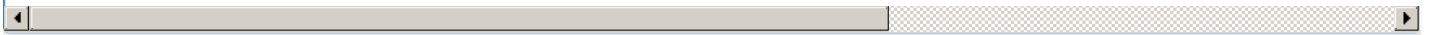
Security Advisory for Pre-authentication Stack Overflow on some Routers and Nighthawk WiFi Mesh Systems, PSV-2022-0146 | Answer | NE

Netgear Nighthawk r7000p aws_json Unauthenticated Double Stack Overflow Vulnerability

www.netgear.com/about/security

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). 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