



CVE-2020-28041

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

Summary

CVE	CVE-2020-28041
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-02 21:15:00 UTC
Updated	2022-10-19 17:17:00 UTC
Description	The SIP ALG implementation on NETGEAR Nighthawk R7000 1.0.9.64_10.2.64 devices allows remote attackers to commu

Risk And Classification

Problem Types: CWE-276

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Nighthawk R7000	-	All	All	All
Hardware	Netgear	Nighthawk R7000	-	All	All	All
Operating System	Netgear	Nighthawk R7000 Firmware	1.0.9.64_10.2.64	All	All	All
Operating System	Netgear	Nighthawk R7000 Firmware	1.0.9.64_10.2.64	All	All	All

References

Reference
Samy Kamkar - NAT Slipstreaming
The attack relies on the ALG ignoring the IP fragment offset in the UDP case onl... Hacker News
GitHub - samyk/slipstream: NAT Slipstreaming allows an attacker to remotely access any TCP/UDP services bound to a victim machine, bypa
Security Advisory
It's not smuggling a SIP session request via HTTP headers - even if it didn't lo... Hacker News
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](#) 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](#)