



CVE-2021-45606

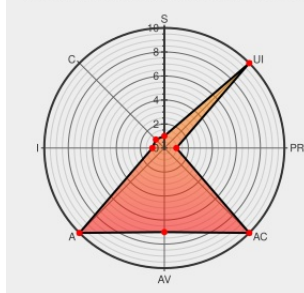
Published on: Not Yet Published

Last Modified on: 01/07/2022 07:21:00 PM UTC

CVE-2021-45606

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AC:L/AV:A/A:H/C:N/I:N/PR:H/S:U/UI:N



Certain versions of **R6400** from **Netgear** contain the following vulnerability:

Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6400 before 1.0.1.70, R7000 before 1.0.11.126, R7900 before 1.0.4.46, R7900P before 1.4.2.84, R7960P before 1.4.2.84, R8000 before 1.0.4.74, R8000P before 1.4.2.84, RAX200 before 1.0.4.120, RS400 before 1.5.1.80, R6400v2 before 1.0.4.118, R7000P before 1.3.3.140, RAX80 before 1.0.4.120, R6700v3 before 1.0.4.118, R6900P before 1.3.3.140, and RAX75 before 1.0.4.120.

CVE-2021-45606 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Advisory for Best Authentication Stack Overflow on		MISC link netgear.com/000064408/Security-Advisory

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Netgear	R6400	-	All	All	All
Hardware 	Netgear	R6400v2	-	All	All	All
Operating System	Netgear	R6400v2 Firmware	All	All	All	All
Operating System	Netgear	R6400 Firmware	All	All	All	All
Hardware 	Netgear	R6700v3	-	All	All	All
Operating System	Netgear	R6700v3 Firmware	All	All	All	All
Hardware 	Netgear	R6900p	-	All	All	All
Operating System	Netgear	R6900p Firmware	All	All	All	All
Hardware 	Netgear	R7000	-	All	All	All
Hardware 	Netgear	R7000p	-	All	All	All
Operating System	Netgear	R7000p Firmware	All	All	All	All
Operating System	Netgear	R7000 Firmware	All	All	All	All
Hardware 	Netgear	R7900	-	All	All	All
Hardware 	Netgear	R7900p	-	All	All	All
Operating System	Netgear	R7900p Firmware	All	All	All	All
Operating System	Netgear	R7900 Firmware	All	All	All	All
Hardware 	Netgear	R7960p	-	All	All	All
Operating System	Netgear	R7960p Firmware	All	All	All	All
Hardware 	Netgear	R8000	-	All	All	All
Hardware 	Netgear	R8000p	-	All	All	All

Operating System	Netgear	R8000p Firmware	All	All	All	All
Operating System	Netgear	R8000 Firmware	All	All	All	All
Hardware	Netgear	Rax200	-	All	All	All
Operating System	Netgear	Rax200 Firmware	All	All	All	All
Hardware	Netgear	Rax75	-	All	All	All
Operating System	Netgear	Rax75 Firmware	All	All	All	All
Hardware	Netgear	Rax80	-	All	All	All
Operating System	Netgear	Rax80 Firmware	All	All	All	All
Hardware	Netgear	Rs400	-	All	All	All
Operating System	Netgear	Rs400 Firmware	All	All	All	All
cpe:2.3:h:netgear:r6400:-:*:*:*:*:*:						
cpe:2.3:h:netgear:r6400v2:-:*:*:*:*:*:						
cpe:2.3:o:netgear:r6400v2_firmware:*:*:*:*:*:						
cpe:2.3:o:netgear:r6400_firmware:*:*:*:*:*:						
cpe:2.3:h:netgear:r6700v3:-:*:*:*:*:*:						
cpe:2.3:o:netgear:r6700v3_firmware:*:*:*:*:*:						
cpe:2.3:h:netgear:r6900p:-:*:*:*:*:*:						
cpe:2.3:o:netgear:r6900p_firmware:*:*:*:*:*:						
cpe:2.3:h:netgear:r7000:-:*:*:*:*:*:						
cpe:2.3:h:netgear:r7000p:-:*:*:*:*:*:						
cpe:2.3:o:netgear:r7000p_firmware:*:*:*:*:*:						
cpe:2.3:o:netgear:r7000_firmware:*:*:*:*:*:						
cpe:2.3:h:netgear:r7900:-:*:*:*:*:*:						
cpe:2.3:h:netgear:r7900p:-:*:*:*:*:*:						
cpe:2.3:o:netgear:r7900p_firmware:*:*:*:*:*:						
cpe:2.3:o:netgear:r7900_firmware:*:*:*:*:*:						
cpe:2.3:h:netgear:r7960p:-:*:*:*:*:*:						

cpe:2.3:o:netgear:r7960p_firmware:~::~::~:
cpe:2.3:h:netgear:r8000:~::~::~:
cpe:2.3:h:netgear:r8000p:~::~::~:
cpe:2.3:o:netgear:r8000p_firmware:~::~::~:
cpe:2.3:o:netgear:r8000_firmware:~::~::~:
cpe:2.3:h:netgear:rax200:~::~::~:
cpe:2.3:o:netgear:rax200_firmware:~::~::~:
cpe:2.3:h:netgear:rax75:~::~::~:
cpe:2.3:o:netgear:rax75_firmware:~::~::~:
cpe:2.3:h:netgear:rax80:~::~::~:
cpe:2.3:o:netgear:rax80_firmware:~::~::~:
cpe:2.3:h:netgear:rs400:~::~::~:
cpe:2.3:o:netgear:rs400_firmware:~::~::~:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
← Previous ID Next ID→		