



CVE-2017-18865

Published on: 05/05/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:55 PM UTC

CVE-2017-18865

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

Certain versions of **R8300** from **Netgear** contain the following vulnerability:

Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R8300 before 1.0.2.104 and R8500 before 1.0.2.104.

CVE-2017-18865 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.8 - MEDIUM**

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

CVSS2 Score: **5.2 - MEDIUM**

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

CVE References

Description	Tags	Link
Security Advisory for Post-Authentication Stack Overflow on R8300 and R8500, PSV-2017-2228 Answer NETGEAR Support	Vendor Advisory kb.netgear.com text/html	N MISC kb.netgear.com/000051485/Security-Advisory-for-Post-Authentication-Stack-Overflow-on-R8300-and-R8500-PSV-2017-2228

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	R8300	-	All	All	All
Hardware 	Netgear	R8300	-	All	All	All
Operating System	Netgear	R8300 Firmware	All	All	All	All
Operating System	Netgear	R8300 Firmware	All	All	All	All
Hardware 	Netgear	R8500	-	All	All	All
Hardware 	Netgear	R8500	-	All	All	All
Operating System	Netgear	R8500 Firmware	All	All	All	All
Operating System	Netgear	R8500 Firmware	All	All	All	All
cpe:2.3:h:netgear:r8300:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:h:netgear:r8300:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:netgear:r8300_firmware:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:netgear:r8300_firmware:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:h:netgear:r8500:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:h:netgear:r8500:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:netgear:r8500_firmware:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:netgear:r8500_firmware:~::~~::~~::~~::~~::~~::~~::						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)