CVE-2018-21173

Published on: 04/27/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:35 PM UTC

CVE-2018-21173

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF

Certain versions of R7500 from Netgear contain the following vulnerability:

Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7500 before 1.0.0.122, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.

CVE-2018-21173 has been assigned by 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 Some Routers, PSV-2017-2627 | Answer | NETGEAR	Vendor Advisory kb.netgear.com	CONFIRM kb.netgear.com/000055185/Security-Advisory-for-Post-Authentication-Stack-Overflow-on-

Support	text/html	Some-Routers-PSV-2017-2627

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	R7500	-	All	All	All
Hardware	Netgear	R7500	-	All	All	All
Operating System	Netgear	R7500 Firmware	All	All	All	All
Operating System	Netgear	R7500 Firmware	All	All	All	All
Hardware	Netgear	R7800	-	All	All	All
Hardware	Netgear	R7800	-	All	All	All
Operating System	Netgear	R7800 Firmware	All	All	All	All
Operating System	Netgear	R7800 Firmware	All	All	All	All
Hardware	Netgear	R9000	-	All	All	All
Hardware	Netgear	R9000	-	All	All	All
Operating System	Netgear	R9000 Firmware	All	All	All	All
Operating System	Netgear	R9000 Firmware	All	All	All	All
Hardware	Netgear	Wndr3700	v4	All	All	All
Hardware	Netgear	Wndr3700	v4	All	All	All
Operating System	Netgear	Wndr3700 Firmware	All	All	All	All
Operating System	Netgear	Wndr3700 Firmware	All	All	All	All
Hardware	Netgear	Wndr4300	-	All	All	All
Hardware	Netgear	Wndr4300	v2	All	All	All
Hardware	Netgear	Wndr4300	-	All	All	All
Hardware	Netgear	Wndr4300	v2	All	All	All
Operating	Netgear	Wndr4300 Firmware	All	All	All	All

System						
Operating System	Netgear	Wndr4300 Firmware	All	All	All	All
Hardware	Netgear	Wndr4500	v3	All	All	All
Hardware	Netgear	Wndr4500	v3	All	All	All
Operating System	Netgear	Wndr4500 Firmware	All	All	All	All
Operating System	Netgear	Wndr4500 Firmware	All	All	All	All
Hardware	Netgear	Wnr2000	v5	All	All	All
Hardware	Netgear	Wnr2000	v5	All	All	All
Operating System	Netgear	Wnr2000 Firmware	All	All	All	All
Operating System	Netgear	Wnr2000 Firmware	All	All	All	All

cpe:2.3:h:netgear:r7500:-:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:r7500:-:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:r7500_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:r7500_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:r7800:-:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:r7800:-:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:r7800_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:r7800_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:r9000:-:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:r9000:-:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:r9000_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:r9000_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:wndr3700:v4:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:wndr3700:v4:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:wndr3700_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:wndr3700_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:wndr4300:-:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:wndr4300:v2:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:wndr4300:-:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:wndr4300:v2:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:wndr4300_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:wndr4300_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:wndr4500:v3:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:wndr4500:v3:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:wndr4500_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:wndr4500_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:wnr2000:v5:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:wnr2000:v5:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:wnr2000_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:wnr2000_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→