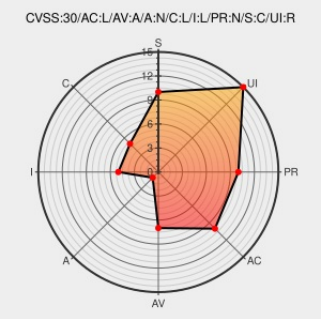
CVE-2017-18701

Published on: 04/24/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:54 PM UTC

CVE-2017-18701

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



Certain versions of R6700 from Netgear contain the following vulnerability:

Certain NETGEAR devices are affected by reflected XSS. This affects R6700 before 1.0.1.36 and R6900 before 1.0.1.34.

CVE-2017-18701 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Security Advisory for Reflected Cross-Site Scripting on Some Routers, PSV-2017-2513 | Answer | NETGEAR Support	Vendor Advisory, kb.netgear.com, text/html	CONFIRM kb.netgear.com/000053201/Security-Advisory-for-Reflected-Cross-Site-Scripting-on-Some-Routers-PSV-2017-2513

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	R6700	-	All	All	All
Hardware	Netgear	R6700	-	All	All	All
Operating System	Netgear	R6700 Firmware	All	All	All	All
Operating System	Netgear	R6700 Firmware	All	All	All	All
Hardware	Netgear	R6900	-	All	All	All
Hardware	Netgear	R6900	-	All	All	All
Operating System	Netgear	R6900 Firmware	All	All	All	All
Operating System	Netgear	R6900 Firmware	All	All	All	All

cpe:2.3:h:netgear:r6700:-:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:r6700:-:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:r6700_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:r6700_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:r6900:-:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:r6900:-:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:r6900_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:r6900_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 registred 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