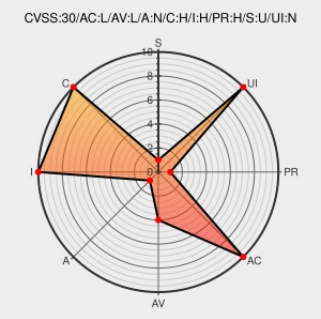
CVE-2019-20662

Published on: 04/15/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:50 PM UTC

CVE-2019-20662

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



Certain versions of Rbk50 from Netgear contain the following vulnerability:

Certain NETGEAR devices are affected by stored XSS. This affects RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and RBK50 before 2.3.5.30.

CVE-2019-20662 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.3 - MEDIUM

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

CVSS2 Score: 2.3 - LOW

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

CVE References

Description	Tags	Link
Security Advisory for Stored Cross Site Scripting on Some WiFi Systems, PSV-2018-0560 | Answer | NETGEAR Support	Vendor Advisory, kb.netgear.com, text/html	CONFIRM kb.netgear.com/000061477/Security-Advisory-for-Stored-Cross-Site-Scripting-on-Some-WiFi-Systems-PSV-2018-0560

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	Rbk50	-	All	All	All
Hardware	Netgear	Rbk50	-	All	All	All
Operating System	Netgear	Rbk50 Firmware	All	All	All	All
Operating System	Netgear	Rbk50 Firmware	All	All	All	All
Hardware	Netgear	Rbr50	-	All	All	All
Hardware	Netgear	Rbr50	-	All	All	All
Operating System	Netgear	Rbr50 Firmware	All	All	All	All
Operating System	Netgear	Rbr50 Firmware	All	All	All	All
Hardware	Netgear	Rbs50	-	All	All	All
Hardware	Netgear	Rbs50	-	All	All	All
Operating System	Netgear	Rbs50 Firmware	All	All	All	All
Operating System	Netgear	Rbs50 Firmware	All	All	All	All

cpe:2.3:h:netgear:rbk50:-:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:rbk50:-:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:rbk50_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:rbk50_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:rbr50:-:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:rbr50:-:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:rbr50_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:rbr50_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:rbs50:-:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:rbs50:-:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:rbs50_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:rbs50_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→