

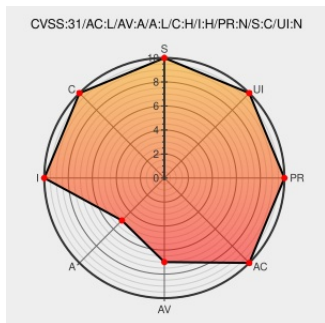


CVE-2020-26906

Published on: 10/09/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-26906

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

Certain versions of [Cbr40](#) from [Netgear](#) contain the following vulnerability:

Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects CBR40 before 2.5.0.10, RBK752 before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBR850 before 3.2.10.11, and RBS850 before 3.2.10.11.

CVE-2020-26906 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
ADJACENT_NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **8.3 - HIGH**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Security Advisory for Admin Credential Disclosure on Some WiFi Systems, PSV-2020-0048 Answer NETGEAR Support	Vendor Advisory kb.netgear.com text/html	N MISC kb.netgear.com/000062348/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0048

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	Cbr40	-	All	All	All
Hardware 	Netgear	Cbr40	-	All	All	All
Operating System	Netgear	Cbr40 Firmware	All	All	All	All
Operating System	Netgear	Cbr40 Firmware	All	All	All	All
Hardware 	Netgear	Rbk752	-	All	All	All
Hardware 	Netgear	Rbk752	-	All	All	All
Operating System	Netgear	Rbk752 Firmware	All	All	All	All
Operating System	Netgear	Rbk752 Firmware	All	All	All	All
Hardware 	Netgear	Rbk852	-	All	All	All
Hardware 	Netgear	Rbk852	-	All	All	All
Operating System	Netgear	Rbk852 Firmware	All	All	All	All
Operating System	Netgear	Rbk852 Firmware	All	All	All	All
Hardware 	Netgear	Rbr750	-	All	All	All
Hardware 	Netgear	Rbr750	-	All	All	All
Operating System	Netgear	Rbr750 Firmware	All	All	All	All
Operating System	Netgear	Rbr750 Firmware	All	All	All	All
Hardware 	Netgear	Rbr850	-	All	All	All
Hardware 	Netgear	Rbr850	-	All	All	All
Operating System	Netgear	Rbr850 Firmware	All	All	All	All
Operating System	Netgear	Rbr850 Firmware	All	All	All	All
Hardware 	Netgear	Rbs750	-	All	All	All

