CVE-2021-29070

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-29070
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-23 07:15:00 UTC
Updated	2021-03-26 18:19:00 UTC
Description	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.17

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Rbk852	-	All	All	All
Operating System	Netgear	Rbk852 Firmware	All	All	All	All
Hardware	Netgear	Rbk853	-	All	All	All
Operating System	Netgear	Rbk853 Firmware	All	All	All	All
Hardware	Netgear	Rbk854	-	All	All	All
Operating System	Netgear	Rbk854 Firmware	All	All	All	All
Hardware	Netgear	Rbr850	-	All	All	All
Operating System	Netgear	Rbr850 Firmware	All	All	All	All
Hardware	Netgear	Rbs850	-	All	All	All
Operating System	Netgear	Rbs850 Firmware	All	All	All	All

References

Reference	Sour
Security Advisory for Post-Authentication Command Injection on Some WiFi Routers, PSV-2020-0530 | Answer | NETGEAR Support	MISC
CVE Program record	CVE.(
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**