CVE-2021-45535

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

Summary

CVE	CVE-2021-45535
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-26 01:15:00 UTC
Updated	2022-01-04 20:44:00 UTC
Description	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RAX200 before 1.0.3.

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Rax200	-	All	All	All
Operating System	Netgear	Rax200 Firmware	All	All	All	All
Hardware	Netgear	Rax75	-	All	All	All
Operating System	Netgear	Rax75 Firmware	All	All	All	All
Hardware	Netgear	Rax80	-	All	All	All
Operating System	Netgear	Rax80 Firmware	All	All	All	All
Hardware	Netgear	Rbk752	-	All	All	All
Hardware	Netgear	Rbk752	-	All	All	All
Hardware	Netgear	Rbk852	-	All	All	All
Operating System	Netgear	Rbk852 Firmware	All	All	All	All
Hardware	Netgear	Rbr750	-	All	All	All
Operating System	Netgear	Rbr750 Firmware	All	All	All	All
Hardware	Netgear	Rbr850	-	All	All	All
Operating System	Netgear	Rbr850 Firmware	All	All	All	All
Hardware	Netgear	Rbs750	-	All	All	All
Operating System	Netgear	Rbs750 Firmware	All	All	All	All
Hardware	Netgear	Rbs850	-	All	All	All

Operating System	Netgear	Rbs850 Firmware	All	All	All	All

References

Reference
Security Advisory for Post-Authentication Command Injection on Some Routers and WiFi Systems, PSV-2020-0052 | Answer | NETGEAR Sup
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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