CVE-2021-38520

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-38520
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-11 00:15:00 UTC
Updated	2021-08-18 20:23:00 UTC
Description	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R6400 before 1.0.1.52

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	R6400	-	All	All	All
Hardware	Netgear	R6400	v2	All	All	All
Operating System	Netgear	R6400 Firmware	All	All	All	All
Hardware	Netgear	R6700	v2	All	All	All
Hardware	Netgear	R6700	v3	All	All	All
Operating System	Netgear	R6700 Firmware	All	All	All	All
Hardware	Netgear	R6900	v2	All	All	All
Operating System	Netgear	R6900 Firmware	All	All	All	All
Hardware	Netgear	R7000p	-	All	All	All
Operating System	Netgear	R7000p Firmware	All	All	All	All

References

Reference	Source
Security Advisory for Post-Authentication Command Injection on Some Routers, PSV-2018-0565 | Answer | NETGEAR Support	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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