



CVE-2022-38452

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-38452
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-21 18:15:00 UTC
Updated	2023-03-29 11:15:00 UTC
Description	A command execution vulnerability exists in the hidden telnet service functionality of Netgear Orbi Router RBR750 4.6.8.5.

Risk And Classification

Problem Types: CWE-912

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Rbs750	-	All	All	All
Operating System	Netgear	Rbs750 Firmware	4.6.8.5	All	All	All

References

Reference	Source
Security Advisory for Post-authentication Command Injection on the RBR750, PSV-2022-0186 Answer NETGEAR Support	MISC
TALOS-2022-1595 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	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.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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