



CVE-2023-4746

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

Summary

CVE	CVE-2023-4746
State	PUBLIC
Assigner	cna@vuldb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-04 01:15:00 UTC
Updated	2023-11-07 04:22:00 UTC
Description	A vulnerability classified as critical has been found in TOTOLINK N200RE V5 9.3.5u.6437_B20230519. This affects the fun

Risk And Classification

Problem Types: CWE-134

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Totolink	N200re-v5	-	All	All	All
Operating System	Totolink	N200re-v5 Firmware	9.3.5u.6437_b20230519	All	All	All

References

Reference	Source
CVE-2023-4746: TOTOLINK N200RE V5 Validity_check format string	MISC
Use format string bypass Totolink's Validity_check function, lead to remote OS command injection (CVE-2023-4746) · GitHub	MISC
Login required	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.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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