



CVE-2023-39745

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

Summary

CVE	CVE-2023-39745
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-21 03:15:00 UTC
Updated	2023-08-25 15:02:00 UTC
Description	TP-Link TL-WR940N V2, TP-Link TL-WR941ND V5 and TP-Link TL-WR841N V8 were discovered to contain a buffer overfl

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tp-link	Tl-wr841n V8	-	All	All	All
Operating System	Tp-link	Tl-wr841n V8 Firmware	-	All	All	All
Hardware	Tp-link	Tl-wr940n V2	-	All	All	All
Operating System	Tp-link	Tl-wr940n V2 Firmware	-	All	All	All
Hardware	Tp-link	Tl-wr941nd V5	-	All	All	All
Operating System	Tp-link	Tl-wr941nd V5 Firmware	-	All	All	All

References

Reference
TP-Link TL-WR940N/TL-WR941ND/TL-WR841N wireless router /userRpm/AccessCtrlAccessRulesRpm buffer read out-of-bounds vulnerability
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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)