

CVE-2023-33538

TP-Link Multiple Routers Command Injection Vulnerability

CISA KEV since Jun 16, 2025

Actively exploited

TP-Link TL-WR940N V2/V4, TL-WR841N V8/V10, and TL-WR740N V1/V2 was discovered to contain a command injection vulnerability via the component /userRpm/WlanNetworkRpm .

EVRS 75 _{/100} Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.416 98.7th percentile · FIRST	CISA DEADLINE Jul 7, 2025 KEV since 2025 · listed over a year
--	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.416 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
tl-wr940n firmware	–	no fixed version listed	NVD
tl-wr841n firmware	–	no fixed version listed	NVD
tl-wr740n firmware	–	no fixed version listed	NVD
tl-wr940n	2.0 4.0	no fixed version listed	NVD
tl-wr841n	8.0 10.0	no fixed version listed	NVD
tl-wr740n	1.0 2.0	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-49g9-8m2w-hfgg
NVD nvd.nist.gov/vuln/detail/CVE-2023-33538
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-37697

tp-link.com tp-link.com/nordic/support/faq/3562/
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnabile.com/vulnerability-management/cve/CVE-2023-33538

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.