

CVE-2025-9377

TP-Link Archer C7(EU) and TL-WR841N/ND(MS) OS Command Injection Vulnerability

CISA KEV since Sep 3, 2025

Actively exploited

The authenticated remote command execution (RCE) vulnerability exists in the Parental Control page on TP-Link Archer C7(EU) V2 and TL-WR841N/ND(MS) V9. This issue affects Archer C7(EU) V2: before 241108 and TL-WR841N/ND(MS) V9: before 241108. Both products have reached the status of EOL (end-of-life). It's recommending to purchase the new product to ensure better performance and security. If replacement is not an option in the short term, please use the second reference link to download and install the patch(es).

EVRS 75_{/100} Urgent priority	CVSS V4.0 8.6 High · NVD	EPSS 0.377 98.5th percentile · FIRST	CISA DEADLINE Sep 24, 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	0.377 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.6	☐ 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-wr841n firmware	< 241108	241108	NVD
tl-wr841nd firmware	< 241108	241108	NVD
archer c7 firmware	< 241108	241108	NVD
tl-wr841n	v9	no fixed version listed	NVD
tl-wr841nd	9	no fixed version listed	NVD
archer c7	2.0	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-37mx-8m3f-j8vm
tp-link.com tp-link.com/us/support/faq/4308/
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2025-9377

Additional guidance tp-link.com/us/support/faq/4365/
NVD nvd.nist.gov/vuln/detail/CVE-2025-9377
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-26234

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