مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Command Injection Vulnerability in Multiple TP-Link Routers

Tracking #:432319194

Date:25-06-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity command injection vulnerability, CVE-2026-11834, has been disclosed in multiple TP-Link router models.

TECHNICAL DETAILS:

A high-severity command injection vulnerability, CVE-2026-11834, has been disclosed in multiple TP-Link router models. The vulnerability resides in the DHCP option processing logic, where insufficient validation of externally supplied DHCP option data may allow an adjacent, unauthenticated attacker to execute arbitrary commands on vulnerable devices.

Vulnerability Details

- CVE ID: CVE-2026-11834
- Vulnerability Type: Command Injection
- CVSS v4.0 Score: 8.7 (High)
- Attack Vector: Adjacent Network (AV)
- Authentication Required: None
- User Interaction: None
- Privileges Required: None

Affected Products

Product	Hardware Version	Fixed Firmware Version
Archer MR200 (EN)	V7	1.3.0 Build 250605
Archer MR200 (EU)	V8	1.5.0 Build 260605
Archer MR402 (EU)	V1	1.5.0 Build 260605
Archer VR2100 (EU)	V1	EU_V1_260330
Archer C20	V5	EU_V5_260317 / US_V5_260419
Archer C20	V6	V6_260608
TL-MR6400 (EU)	V7	1.7.0 Build 260413

RECOMMENDATIONS:

Immediate Actions:

- Upgrade all affected TP-Link routers to the latest firmware versions provided by TP-Link**.**

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.tp-link.com/us/support/faq/5141/