مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Command Injection Vulnerability in TP-Link Telnet CLI

Tracking #:432318601

Date:15-03-2026

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

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a high-severity command injection vulnerability identified as CVE-2026-3841 affects TP-Link TL-MR6400 routers running specific firmware versions.

TECHNICAL DETAILS:

A high-severity command injection vulnerability identified as CVE-2026-3841 affects TP-Link TL-MR6400 routers running specific firmware versions. The vulnerability exists in the Telnet command-line interface (CLI) due to insufficient sanitization of user-supplied input during certain CLI operations. An authenticated attacker with elevated privileges could exploit the flaw to execute arbitrary system commands on the device.

Vulnerability Information

- CVE ID: CVE-2026-3841
- Affected Product: TP-Link TL-MR6400
- Vulnerability Type: Command Injection
- Attack Vector: Adjacent Network (Telnet interface)
- CVSS v4.0 Score: 8.5 (High)

Affected Products and Versions

- TP-Link TL-MR6400 v5.3-Versions earlier than 1.9.0 Build 260108

RECOMMENDATIONS:

Patch Management

- Upgrade firmware of affected routers to fixed or latest version 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/5016/