مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

DoS Vulnerability in TP-Link TL-WR841N Router

Tracking #:432318677

Date:29-03-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a high-severity vulnerability has been identified in the UPnP component of the TP-Link TL-WR841N router.

TECHNICAL DETAILS:

A high-severity vulnerability has been identified in the UPnP component of the TP-Link TL-WR841N router Tracked as CVE-2026-3622, the flaw arises from improper input validation, which can be exploited to trigger an out-of-bounds read condition. Successful exploitation may crash the UPnP service, resulting in a denial-of-service (DoS) condition.

Vulnerability Details:

- CVE ID: CVE-2026-3622
- Severity: High (CVSS v4.0: 7.1)
- CVSS Vector: CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
- Vulnerability Type: Out-of-Bounds Read
- Component Affected: UPnP (Universal Plug and Play)

Affected Products

- Product: TP-Link TL-WR841N
- Hardware Version: v14

Affected Firmware Versions

- EN Firmware:
  - < EN_0.9.1 4.19 Build 260303 Rel.42399n (V14_260303)
- US Firmware:
  - < US_0.9.1.4.19 Build 260312 Rel.49108n (V14_0304)

Temporary Workaround

- Disable UPnP if not strictly required
  - Reduces attack surface significantly
  - Prevents exploitation via UPnP interface

RECOMMENDATIONS:

- Immediate Remediation
  - Upgrade to the latest firmware 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/5033/