مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Denial-of-Service (DoS) Vulnerability in TP-Link Routers

Tracking #:432318046

Date:21-11-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity Denial-of-Service (DoS) vulnerability (CVE-2025-11676) has been identified in the TP-Link TL-WR940N V6 wireless router.

TECHNICAL DETAILS:

A high-severity Denial-of-Service (DoS) vulnerability (CVE-2025-11676) has been identified in the TP-Link TL-WR940N V6 wireless router, affecting all firmware versions up to and including Build 220801. The flaw resides in the router's Universal Plug and Play (UPnP) module, where improper input validation may allow an unauthenticated, adjacent-network attacker to crash the UPnP service. Exploitation of this vulnerability results in the UPnP service becoming unavailable, potentially disrupting automatic port-forwarding operations and other network functions dependent on UPnP. TP-Link has released patched firmware (Build 250919 and Build 250925) addressing this vulnerability.

Vulnerability Details:

- CVE-2025-11676
- CVSS v4.0 Score: 7.1 / High
- The vulnerability is caused by improper input validation within the UPnP modules of the TP-Link TL-WR940N V6 router. An attacker with access to the adjacent network can send crafted UPnP packets to the target device. Due to insufficient validation, these packets may trigger a state that causes the UPnP service to crash, resulting in a Denial-of-Service (DoS) condition.

Affected & Fixed Versions:

Product Model	Affected Version	Fixed Version
TL-WR940N V6	≤ Build 220801	Build 250919, Build 250925

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update TL-WR940N V6 to the latest firmware.

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/4755/