مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Stored Cross-Site Scripting (XSS) Vulnerability in TP-Link Routers

Tracking #:432317103

Date:22-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a stored Cross-Site Scripting (XSS) vulnerability has been discovered in the web interface of the TP-Link WR841N router that allows remote attackers to execute arbitrary JavaScript code, potentially compromising administrator credentials and router security.

TECHNICAL DETAILS:

A stored Cross-Site Scripting (XSS) vulnerability has been discovered in the web interface of the TP-Link WR841N router, specifically impacting versions v14, v14.6, and v14.8 up to firmware build 241230 Rel. 50788n. This vulnerability allows a remote unauthenticated attacker on the same network to inject malicious JavaScript code via the port mapping description on the upnp.htm page. When an administrator later visits this page, the malicious script executes in the context of the admin's browser, potentially leading to unauthorized actions such as stealing login credentials or modifying router settings.

Vulnerability Details:

- CVE ID: CVE-2025-25427
- CVSS v4.0 Score: 8.6 (High)
- Affected Devices: TP-Link WR841N v14/v14.6/v14.8 <= Build 241230 Rel. 50788n
- Risk: Remote attackers can inject malicious JavaScript via the UPnP port mapping description, leading to code execution when the UPnP page is loaded. This could enable credential theft, DNS hijacking, or unauthorized configuration changes.
- Patched Version: Build 250328 Rel.49245n

RECOMMENDATIONS:

- Download the latest firmware from TP-Link's official support portal.
- After updating, change the administrator password to ensure any leaked credentials cannot be reused.

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/4415/