مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

RCE Vulnerability in TP-Link AX Series Routers

Tracking #:432317675

Date:08-09-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability (CVE-2025-9961) has been identified in the CWMP binary of TP-Link Archer AX10 and Archer AX1500 series routers.

TECHNICAL DETAILS:

A high-severity vulnerability (CVE-2025-9961) has been identified in the CWMP binary of TP-Link Archer AX10 and Archer AX1500 series routers. An authenticated attacker can exploit this flaw to execute arbitrary code remotely. Although the CWMP function is disabled by default, attackers who successfully position themselves in a Man-In-The-Middle (MITM) attack scenario can trigger exploitation.

Vulnerability Details

- Vulnerability ID: CVE-2025-9961
- CVSS v4.0 Score: 8.6 (High)
- Vulnerability Type: Authenticated Remote Code Execution (RCE)
- Vector: Exploitable via CWMP binary (requires authentication + MITM)
- Affected Function: CWMP (disabled by default)
- Impact: High – Potential arbitrary code execution

Product Model	Related Vulnerability	Affected Versions	Fixed Versions
Archer AX10	CVE-2025-9961	Firmware < 1.2.1	Firmware ≥ 1.2.1
Archer AX1500	CVE-2025-9961	Firmware < 1.3.11	Firmware ≥ 1.3.12

RECOMMENDATIONS:

- Immediate Firmware Updates: Update to the latest firmware to fix the vulnerabilities.
- Disable CWMP if not required: Since CWMP is disabled by default, organizations should ensure it remains disabled to reduce attack surface.

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/4647/