مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in TP-Link Tapo Devices

Tracking #:432318889

Date:04-05-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability, tracked as CVE-2025-15557, has been identified in TP-Link Tapo H100 v1 and Tapo P100 v1 devices.

TECHNICAL DETAILS:

A high-severity vulnerability, tracked as CVE-2025-15557, has been identified in TP-Link Tapo H100 v1 and Tapo P100 v1 devices. The flaw arises from improper certificate validation during device-to-cloud communication, allowing an attacker positioned on the same network to intercept and manipulate encrypted traffic.

Vulnerability Details

- Vulnerability ID: CVE-2025-15557
- Vulnerability Type: Improper Certificate Validation
- CVSS v4.0 Score: 7.5 (High)
- Attack Vector: Adjacent Network (same network segment required)
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: Passive (limited interaction required)

Affected Versions

- TP-Link Tapo H100 v1< 1.6.1
- TP-Link Tapo P100 v1< 1.2.6

RECOMMENDATIONS:

- Update Firmware immediately to patched versions.

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/en/support/faq/4949/