مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Root Access Vulnerability in TP-link Devices

Tracking #:432317760

Date:30-09-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability has been identified in the TP-Link Tapo D230S1 that may allow an attacker with physical access to the device to obtain root privileges via UART (Universal Asynchronous Receiver-Transmitter) access.

TECHNICAL DETAILS:

A vulnerability has been identified in the TP-Link Tapo D230S1 (V1.20 firmware versions prior to 1.2.2 Build 20250907) that may allow an attacker with physical access to the device to obtain root privileges via UART (Universal Asynchronous Receiver-Transmitter) access. Successful exploitation enables full control over the device, potentially exposing sensitive data and allowing the device to be weaponized in larger attacks.

Although this vulnerability requires local, physical access and does not pose a direct remote exploitation threat, it remains a high-severity issue due to the impact of unrestricted root-level compromise.

Vulnerability Details

- **Vulnerability ID:** CVE-2025-10991
- **Vulnerability Description:** Attackers with physical access to the Tapo D230S1 smart device may exploit an exposed UART interface to gain root access.
- **Attack Vector:** Physical (AV:P)
- **Impact:**
  - **Confidentiality:** High (VC:H) – attacker gains access to all stored/processed data.
  - **Integrity:** High (VI:H) – attacker can modify device behavior and firmware.
  - **Availability:** High (VA:H) – attacker can disable or brick the device.
- **CVSS v4.0 Base Score:** 7.0 (High)
- **Affected Products/Versions:** Tapo D230S1 V1.20 - < 1.2.2 Build 20250907
- **Fixed Version-**1.2.2 Build 20250907

RECOMMENDATIONS:

- Update Firmware Immediately: Upgrade affected devices to fixed firmware version or later.

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.

REFERNCES:

- https://www.tp-link.com/us/support/faq/4693/