efchatz Rename Web/TP-Link/CVE-2022-41540/README.md to Web/... ... on Oct 19 History

..

README.md last month

README.md

Vulnerabitily type

Use of Hard-coded cryptographic keys (CVE-2022-41540)

Vendor

TP-Link

Product

AX10v1 V1_211117

Affected component

The web app client uses static cryptographic keys to communicate with the router.

Attack vector

An attacker with a Man-in-the-middle position can capture the relevant traffic between the client and the web app. Then, they can visit the web app login page to gain access to the same cryptographic keys the victim used to communicate with the web app. All keys have the same value, but the sequence key. The latter is a 9-digit key that can be easily brute-forced. So, by using an offline brute force attack an attacker can gain access to encrypted and sensitive information, by decrypting it.

Patch

V1_220401

PoC

replay-offline-tp-link_vFQcNDCv.mp4