

main easy-exploits / Web / TP-Link / Replay /



efchatz Rename Web/TP-Link/CVE-2022-41541/README.md to Web/...

...

on Oct 19

History

..



README.md

last month

☰ README.md

## Vulnerability type

Replay attack (CVE-2022-41541)

## Vendor

TP-Link

## Product

AX10v1 V1\_211117

## Affected component

The web app authentication method accepts a replayed HTTP packet which contains a login message that was previously got accepted by the app.

## Attack vector

A Man-in-the-middle attacker who captures the traffic between the web app and the victim, can escalate a Replay attack, with a previously transmitted encrypted authentication message and gain a valid authentication token. This will allow the attacker to login as an admin user to the application.

# Patch

V1\_220401

# PoC

🔍 replay-active-tp-link\_Ktu2kFUg.mp4 ▾

0:00 / 0:45