Home » Posts

TP-Link's Archer C5v Improper Authorization

February 3, 2021 · 1 min · Gökay

Cve: CVE-2021-27210

TP-Link's Archer C5v stores the all credentials, including the root's credential, in clear text on the device

This vulnerability can be exploited by any authenticated user, even if not authorized, on the local network to access all credentials.

The following HTTP request can be sent to retrieve the data:

If an attacker uses the weak cryptography vulnerability discussed in another blog post, any user on the network can obtain both the credentials of a logged-in user and also all root privileges on the router.





© 2022 Gökay Atar Personel Blog Powered by Hugo & PaperMod