Home » Posts

TP-Link Archer C5v Base64 Cookie

February 3, 2021 · 1 min · Gökay

Cve: CVE-2021-27209

Model: TP-Link Archer C5v

Firmware Version: v1.7_181221

Hardware Version: Archer C5v v1 00000000

Archer C5v stores the authenticated user's credential information within the management interface's cookie by encoding it with base64. When the cookie is decoded, the user's username and password can be accessed in cleartext.

Archer C5v does not use SSL by default in the management interface. Therefore, an attacker on the local network can monitor the traffic and capture the cookie, granting the attacker access to the management interface.
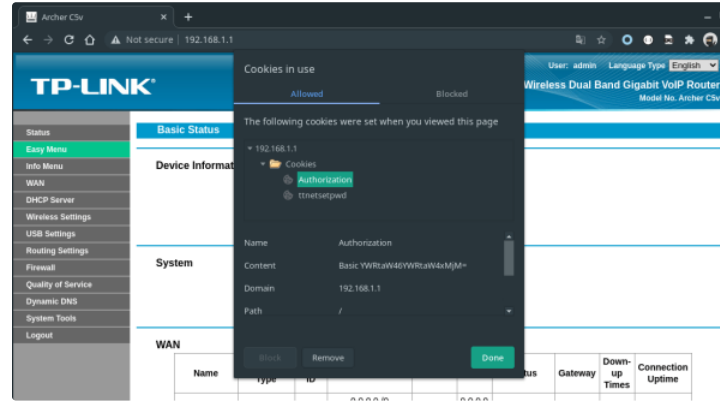
« PREV PAGE

TP-Link's Archer C5v Improper Authorization

NEXT PAGE »

Linux Bash Aktivitelerinin Loglanması