

Leakage of Admin Web-Portal Credential

Make: TP-Link

Model: TL-WR845N

The credentials used in the firmware versions are allowed by default in the upgraded version. The attacker who has captured the credentials during the usage of older firmware usage, can login into the upgraded versions. This problem is applicable to the firmware versions, TL-WR845N(UN)_V4_190219, TL-WR845N(UN)_V4_200909, TL-WR845N(UN)_V4_201214. Below are the steps that can be used to gain the Admin access, even updated to secure firmware versions.

1. An authorized user connects to the TL-WR845N wifi router through a LAN or a wireless network.
2. An attacker also connected to the network with known network connection credentials.
3. Admin Web-Portal credentials disclosure
 - 3.1 TL-WR845N(UN)_V4_190219 [Exploit linked with the MITRE reserved CVE-2024-46341 of our finding]
 - Access the admin web portal of the router by entering the credential.
 - During the above processes, an attacker who is already in the network can sniff the packets that are flowing between the authorized admin and access point/router by performing ARP poisoning.
 - A HTTP POST method packet sent by the authorized admin to the Access Point contains username and password in the cookies (Basic Authorization) of HTTP request in base64 encoded. An attacker can filter this packet, collect and decode the credentials for the further exploit [TL-WR845N(UN)_V4_190219].
 - 3.2 TL-WR845N(UN)_V4_200909, and TL-WR845N(UN)_V4_201214 [Exploit linked with the MITRE reserved CVE-2024-46340 of our finding]
 - During the factory reset in versions TL-WR845N(UN)_V4_200909, TL-WR845N(UN)_V4_201214, the credentials were shared in the plain text.
 - During the above processes, an attacker who is already in the network can sniff the packets that are flowing between the authorized admin and access point/router by performing ARP poisoning.
 - An attacker can filter the packet containing the credentials in plain text.
- Note:** To get the exact packet from the wireshark captured packets, apply the “**http.request.method==POST**” filter. It can also be filtered from the captured .pcapng file [attached]. *Example packet-* The plain-text credentials can be found in the “/cgi/softup HTTP/1.1” packet.
4. An authorized user starts the firmware upgrade process from TL-WR845N(UN)_V4_190219 to TL-WR845N(UN)_V4_200909 or from TL-WR845N(UN)_V4_190219 to TL-WR845N(UN)_V4_201214 or from

TL-WR845N(UN)_V4_200909 to TL-WR845N(UN)_V4_201214. [Upgrade including the latest beta version shared with us]

5. The updated firmware does not prompt users to update the credentials. Even though later firmware versions could ensure secure communication of credentials, already used credentials in the old firmware by default to be used in the updated one. In this case, attackers are already holding the credentials and can get full admin access to the access point/router's web admin portal.

Contributor Name(s): Deven Lunkad, Swaroop Dora, Ashutosh Kumar, and S. Venkatesan (IoT Security Research Lab, Indian Institute of Information Technology, Allahabad, India)

Attachments:

1. Exploit video (Google Drive Link): [BasicAuth_AllVersions.mp4](#)
2. Snapshot of the credential disclosure in the below figure 1.

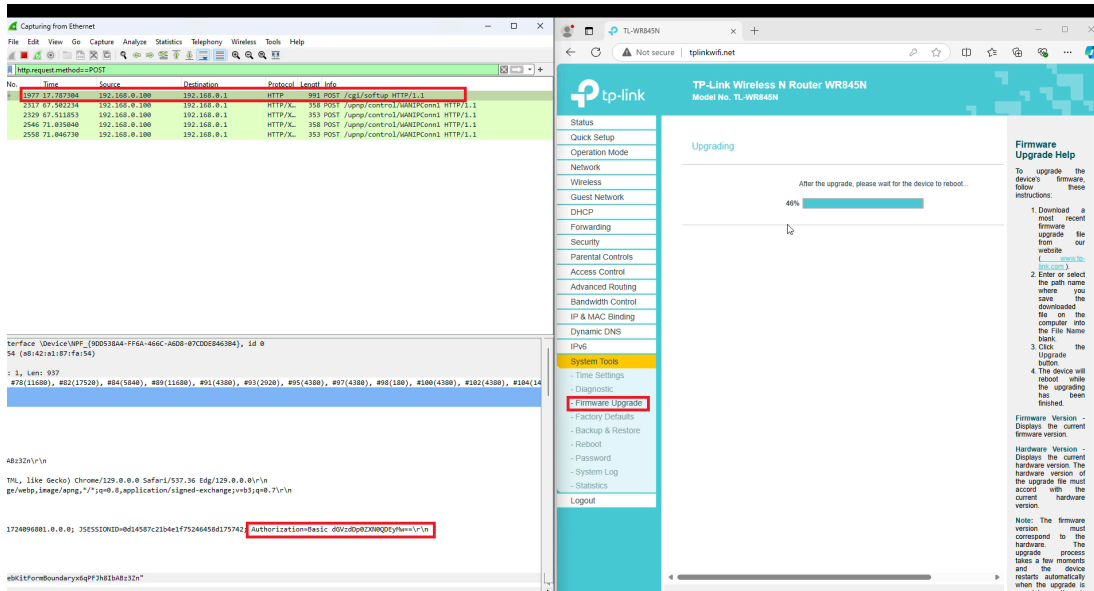


Figure-1: Wireshark image of the credential disclosure packet