Revealing Root Shell Credential

Make: TP-Link
Model: TL-WR845N

This vulnerability is about revealing the "root-shell credentials" present in the firmware of TL-WR845N router. The firmware can be extracted through two methods: SPI Flash memory and manufacturer's public repository (https://www.tp-link.com/in/support/download/tl-wr845n/#Firmware).

After extracting the firmware, we can use tools like *binwalk* or *FirmAudit* (our tool) to extract the files. The MD-5 hashed password is stored in the "*squashfs-root/etc/passwd*" and "*squashfs-root/etc/passwd.bak*" files. The hashed root password can be easily cracked to reveal it as "*1234*" while the root username is in plain-text i.e. "*admin*".

This vulnerability is present in all the firmware versions (TL-WR845N(UN)_V4_190219, TL-WR845N(UN)_V4_200909 and TL-WR845N(UN)_V4_201214) available on the official website of the manufacturer and can be exploited since it gives access to the root user privilege.

Following are the steps to exploit the vulnerability.

1. An unauthorized user can get physical access to the TL-WR845N wifi router's firmware through an SPI flash memory or can download from the official website of the vendor.
2. The binary firmware file can be analyzed using Binwalk or FirmAudit (our tool) to extract the available files in the readable format.
   Command for extraction: *$ binwalk -e firmware.bin*
3. Once extracted all the files, one can head to the *squashfs-root/etc* directory where "passwd" and "passwd.bak" files can be accessed.
4. The username and hashed password can be found in above mentioned files using the following commands:
   Command: *$cat passwd or $ cat passwd.bak*
5. The root user name can be found as "*admin*" in the plain-text format.
6. The password to access the root shell can be found in MD5 hash format which can be easily cracked to reveal it as "*1234*" using any tools i.e., hashcat or john the ripper.
7. To validate the extracted credentials to access the root shell, one can use UART port communication. An interrupt (any key press) must be given before entering the below command.
   Command: *$ login.*
8. After entering the above command, the root shell will prompt for root username and password. Thus, the above credential can be validated.

Contributor Name(s): Akash Singh, Parth Chaurasia, Swaroop Dora, Ashutosh Kumar, and S. Venkatesan (IoT Security Research Lab, Indian Institute of Information Technology, Allahabad, Prayagraj, India.)

Attachments:

1. Exploit video (Google Drive Link): root shell credentials.mp4
2. Snapshot of the credential disclosure in the below figure 1.

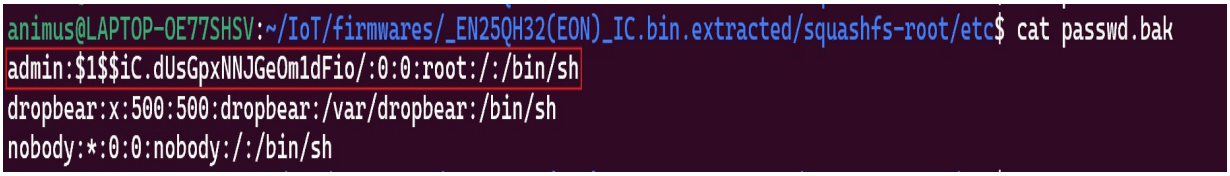

Figure-1: Snapshot of the credential disclosure.