



Reverse Engineering (REV3)

UE 05 – Firmware Analyse – Protokoll

Jakob Mayr

WS 2023/2024

File-Beschaffung

Die benötigte Firmware-Version kann direkt auf der netgear-Seite heruntergeladen werden:

https://www.downloads.netgear.com/files/GDC/R6400/R6400-V1.0.1.12_1.0.11.zip

Analyse Teilkomponenten

Extrahieren des .zip-Archivs:

```
mendacium@fedora ~$ build > REV3UE05-Tools
7z x R6400-V1.0.1.12_1.0.11.zip
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,16 CPUs AMD Ryzen 7
5800U with Radeon Graphics (A50F00),ASM,AES-NI)

Scanning the drive for archives:
1 file, 27537183 bytes (27 MiB)

Extracting archive: R6400-V1.0.1.12_1.0.11.zip
--
Path = R6400-V1.0.1.12_1.0.11.zip
Type = zip
Physical Size = 27537183

Everything is Ok

Files: 2
Size: 27543800
Compressed: 27537183
time:2ms
```

Die Ausführung des Befehls `binwalk` mit der Option `--signature` auf die Datei `r6400-V1.0.1.12_1.0.11.chk` liefert folgende Informationen über die Binärdatei der Firmware:

```
mendacium@kali-mendacium: ~/build/REV3
$ binwalk --signature --tera R6400-V1.0.1.12_1.0.11.chk
DECIMAL      HEXADECIMAL    DESCRIPTION
58           0x3A          TRX firmware header, little endian, image size: 27537408 bytes, CRC32: 0x54507561, flags: 0x0, version: 1, header size: 28 bytes, loader offset: 0x1C, linux kernel offset: 0x20AC00, rootfs offset: 0x0
86           0x56          LZMA compressed data, properties: 0x5D, dictionary size: 65536 bytes, uncompressed size: 5246752 bytes
2141338      0x20AC9A      Squashfs filesystem, little endian, version 4.0, compression:xz, size: 25391589 bytes, 1402 inodes, blocksize: 131072 bytes, created: 2016-05-31 15:57:09
time:83ms
```

- **TRX Firmware-Header:** Das Binärbild enthält einen TRX Firmware-Header, der häufig bei Firmware-Dateien für Router oder ähnliche Geräte verwendet wird. Er ist in Little-Endian-Format mit einer Größe des Images von 27.537.408 Bytes und enthält einen CRC32-Prüfsummenwert. Betrachtet man den Bootloader an Stelle `0x1C` ("loader offset"), so findet man zu Beginn einen String `"U12H332T00_NETGEARHDR0.0"` (radare2 visual mode). Dies könnte eine Information über Name/Version des Bootloaders darstellen:

```
[0x0000001c [xadv]0x 1264 build/REV3UE05-Tools/R6400-V1.0.1.12_1.0.11.chk]> xc @ rlp
- offset - 1C10 1E1F 2021 2223 2425 2627 2829 2A2B CDEF0123456789AB comment
0x0000001c 0000 0000 72ed 1bc7 15dd 0b2c 5531 3248 .....U12H ; rlp ; arg3 ; arg1 ; arg3 ; arg2
0x0000002c 3333 3254 3030 5f4e 4554 4745 4152 4844 332T00_NETGEARHD ; arg3
0x0000003c 5230 0030 a401 6175 5854 0000 0100 1c00 R0.0..auPT..... ; arg4
0x0000004c 0000 60ac 2000 0000 0000 5d00 0001 0020 .....].....
0x0000005c 0f50 0000 0000 0000 69bc 02e 3568 b600 .P.....L...Sh..
0x0000006c f976 6959 866f 63d5 f3bd 5519 3798 0565 .vlf.oc...U.7..e
```

- **LZMA komprimierte Daten:** Der Teil der Datei enthält LZMA-komprimierte Daten. Dies schließt Eigenschaften, eine Wörterbuchgröße und die unkomprimierte Größe ein.
- **Squashfs-Dateisystem:** Das Binärbild umfasst ein Squashfs-Dateisystem. Squashfs ist ein komprimiertes, schreibgeschütztes Dateisystem für Linux. Die Version, der Kompressionstyp (xz), die Größe, die Anzahl der Inodes, die Blockgröße und das Erstellungsdatum werden ebenfalls angegeben.

Das Erstellungsdatum des Squashfs-Dateisystems ist der 31. Mai 2016 um 15:57:09 Uhr.

Extrahieren der LZMA komprimierten Datei und des squashfs-Dateisystems:

```
mendacium@kali-mendacium: ~/build/REV3
$ dd if=R6400-V1.0.1.12_1.0.11.chk of=lzma skip=86 bs=1 count=2141252
2141252+0 records in
2141252+0 records out
2141252 bytes (2.1 MB, 2.0 MiB) copied, 6.36765 s, 336 kB/s

mendacium@kali-mendacium: ~/build/REV3
$ dd if=R6400-V1.0.1.12_1.0.11.chk of=filesystem skip=2141338 bs=1
25396128+0 records in
25396128+0 records out
25396128 bytes (25 MB, 24 MiB) copied, 76.0239 s, 334 kB/s
```

”Mounten” des Dateisystems in ”/mnt”:

```
mendacium@kali-mendacium: ~/build/REV3
└─$ ls
R6400-V1.0.1.12_1.0.11.chk  binwalk  lzma
R6400-V1.0.1.12_1.0.11.chk  filesystem
'R6400-V1.0.1.12_1.0.11.Release Notes.html'  headers

└─$ ls /mnt

└─$ sudo mount -t squashfs -o loop filesystem /mnt/

└─$ ls /mnt
bin  dev  etc  lib  media  mnt  opt  proc  sbin  share  sys  tmp  usr  var  www

└─$
```

Suchen und finden der ”httpd”-Binärdatei:

```
(mendacium@kali-mendacium)-[~/build/REV3]
└─$ sudo find /mnt -name "httpd"
/mnt/usr/sbin/httpd
```

httpd

Informationen (radare2) über die Binärdatei:

```
[0x000000fc]> i
fd      5
file    httpd
size    0x16c4c
humansz 1.4M
mode    r-x
format  elf
iordw   false
block   0x100
type    EXEC (Executable file)
arch     arm
haddr   0x8000
binsz   1692530
hintype  elf
bits    32
canary   false
class    ELF32
compiler GCC (GNU) 3.3.2 20031005 (Debian prerelease) GCC (Buildroot 2012.02) 4.5.3
flags    0x5000002
abi      eabi5
crypto   false
endian   little
havecode true
interp  /lib/ld-uClibc.so.0
laddr    0x0
lang     c
linenum  false
lsyms    false
machine  ARM
nx        true
os        linux
pic       false
relocs    false
relro     no
rpath     NONE
sanitize  false
static    false
stripped  true
subsys    linux
vs         true
va         true
[0x000000fc]> |
```