README.md

Owfuzz

Owfuzz: a WiFi protocol fuzzing tool using openwifi

Discovered vulnerabilities

- CVE-2021-34173
- CVE-2021-34174
- CVE-2021-1903
- CVE-2021-30310
- CVE-2021-33028(Undisclosed)
- CVE-2021-33029(Undisclosed)
- Qualcomm Vulnerbilities

CVE-2021-34173

An attacker can cause a Wi-Fi Denial of Service(DoS) and kernel panic in v4.2 and earlier versions of Espressif's esp32 via a malformated beacon CSA frame. Esp32 device requires a reboot to recover.

- Crash logs

```
I (3494) wifi station: got ip:192.168.50.242
I (3504) wifi station: connected to ap SSID:AS password:1234567890/
Guru Meditation Error: Core  0 panic'ed (LoadProhibited). Exception was unhandled.

Core  0 register dump:
PC      : 0x400f2319  PS      : 0x00060b30  A0      : 0x8008e499  A1      : 0x3ffc0f40
0x400f2319: ieee80211_recv_bar at ??:?

A2      : 0x3ffb5428  A3      : 0x3ffb92cc  A4      : 0x00000088  A5      : 0x00000018
A6      : 0x00000001  A7      : 0x00000000  A8      : 0x3ffb5448  A9      : 0x3ffb9344
A10     : 0x3ffb5428  A11     : 0x03000000  A12     : 0x00000011  A13     : 0x3ffbf010
A14     : 0x40084294  A15     : 0x80000000  SAR     : 0x00000020  EXCCAUSE: 0x0000001c
0x40084294: task_ms_to_tick_wrapper at /Users/sc3d4r/Environment/esp/esp-idf/components/esp_wifi/esp32/esp_adapter.c:401

EXCVADDR: 0x03000000  LBEG    : 0x4000c2e0  LEND    : 0x4000c2f6  LCOUNT  : 0xffffffff

Backtrace:0x400f2316:0x3ffc0f40 0x4008e496:0x3ffc0f60 0x4008e525:0x3ffc0fb0 0x400923b1:0x3ffc0fd0 0x400900f8:0x3ffc0ff0
0x40089f75:0x3ffc1020
0x400f2316: ieee80211_recv_bar at ??:?

0x4008e496: sta_input at ??:?

0x4008e525: sta_rx_cb at ??:?

0x400923b1: ppRxPkt at ??:?

0x400900f8: ppTask at ??:?

0x40089f75: vPortTaskWrapper at /Users/sc3d4r/Environment/esp/esp-idf/components/freertos/port/xtensa/port.c:168

ELF file SHA256: 20d93a4b64d36560

Rebooting...
Re-enable cpu cache.
Guru Meditation Error: Core  0 panic'ed (IllegalInstruction). Exception was unhandled.
Memory dump at 0x400e9e5c: 2e0856e1 09ad6da9 9802d222
0x400e9e5c: rtc_clk_cpu_freq_to_xtal at /Users/sc3d4r/Environment/esp/esp-idf/components/esp_hw_support/port/esp32/rtc_clk.c:439

Core  0 register dump:
PC      : 0x400e9e62  PS      : 0x00060833  A0      : 0x800876a0  A1      : 0x3ffc0d40
0x400e9e62: rtc_clk_cpu_freq_set_xtal at /Users/sc3d4r/Environment/esp/esp-idf/components/esp_hw_support/port/esp32/rtc_clk.c:510

A2      : 0x00000000  A3      : 0x3ff000c4  A4      : 0x00000000  A5      : 0x00000001
A6      : 0x3ffb92cc  A7
0x400817a6: _xt_user_exc at /Users/sc3d4r/Environment/esp/esp-idf/components/freertos/port/xtensa/xtensa_vectors.S:697
```

```
0x400f2316: ieee80211_recv_bar at ??:?

0x4008e496: sta_input at ??:?

0x4008e525: sta_rx_cb at ??:?

0x400923b1: ppRxPkt at ??:?

0x400900f8: ppTask at ??:?

0x40089f75: vPortTaskWrapper at /Users/sc3d4r/Environment/esp/esp-idf/components/freertos/port/xtensa/port.c:168
```

CVE-2021-34174

This vulnerability is discovered in broadcom's BCM4352 and BCM43684 chips. Any wireless router using BCM4352 and BCM43684 will be affected, such as ASUS AX6100. An attacker may cause a Denial of Service (DoS) to any device connected to BCM4352 or BCM43684 routers by an association or reassociation frame.

Qualcomm-Vulnerbilities

- Snapdragon series
- Killer Wireless AC 1535
- QCA9005

Please see [pocs] dir.

Reproduce

```
(1) Linux (ubuntu/kali) OS

    apt-get install pkg-config libnl-3-dev libnl-genl-3-dev libpcap-dev
    git clone https://github.com/aircrack-ng/mdk4
    cd mdk4
    make

    cd src

    #Write payload into ./pocs/poc_test
    echo "payload hex str" > ./pocs/poc_test


(2) Reproducing this issue
    a. Connecting device to AP
    b. To see what channel the AP is working on
    c. To see the MAC address of the AP and the device
    d. Plugging a WiFi USB adapter(support monitor mode and packet injection, 2.4G/5G) into the PC(linux) and to see the usb wifi
interface name.

        sudo ifconfig iface_name down
        sudo iwconfig iface_name mode monitor
        sudo ifconfig iface_name up

    e. Reproduce using mdk4: sudo mdk4 [iface_name] x -c [channel_numer] -v poc_test -s 1 -B [ap-mac] -S [ap-mac] -T [sta-mac]
```

Releases

No releases published

Packages

No packages published