Products

What's new

Services

Publications

Resources

Follow @Openwall on Twitter for new release announcements and other news [prev] [next>] [<thread-prev] [thread-next>] [day] [month] [year] [list]

Date: Thu, 13 Oct 2022 19:13:11 +0200

From: Sönke Huster <shuster@...moo.tu-darmstadt.de>

To: Marcus Meissner <meissner@...e.de>, oss-security@...ts.openwall.com Subject: Re: Various Linux Kernel WLAN security issues (RCE/DOS) found

Hi everyone,

In the following, I quickly introduce the PoC and briefly describe each CVE.

Please see attached:

- \* The PCAP files containing the Wifi frames triggering the vulnerabilities and
- $^{\star}$  inject-pcap.c to inject the Wifi frames into the 802.11 stack
- \* A complete log for each CVE

Thanks to Johannes Berg, who provided the inject-pcap.c script, quickly worked on all the patches and resolved the issues!

The PoC uses mac80211\_hwsim to inject the frames, but the vulnerabilities are - to my knowledge - driver-independent, and we assume that they are exploitable over the air. All the malformed frames are Beacon frames.

# PoC Execution

```
Boot a kernel with mac80211 hwsim included or load the module. Install libnl-3.0 libnl-genl-3.0 libpcap, which is required by the PoC, and compile it as follows:
```

cc -o inject-pcap inject-pcap.c \$(pkg-config --cflags --libs libnl-3.0 libnl-genl-3.0 libpcap)

Afterward, trigger a scan so that the device can receive the frame(s):

iw wlan0 scan trigger

Now, run inject-pcap with the PCAP file as argument.

# CVE-2022-41674

This vulnerability was introduced in v5.1-rc1 and leads to a heap overflow. Compiled with CONFIG SLUB DEBUG ON the kernel emits the following among other errors:

. . .

BUG kmalloc-64 (Tainted: G B ): Left Redzone overwritten

\_\_\_\_\_\_

Object 0xffff8880112b1e40 @offset=3648 fp=0xffff8880112b1f40

Pac

With the fix applied, the payload triggers slab-out-of-bounds. As that specific one is not considered harmful, no additional CVE is assigned, but it is fixed in "wifi: cfg80211: ensure length byte is present

## before access". # CVE-2022-42719 This vulnerability was introduced in v5.2-rc1. With the patch for CVE-2022-41674 and the one mentioned prior applied, the same payload triggers use-afterfrees, such as the following: \_\_\_\_\_\_ BUG: KASAN: use-after-free in ieee80211 update bss from elems (net/mac80211/scan.c:104) Read of size 1 at addr ffff88800befa00a by task ksoftirqd/1/20 # CVE-2022-42720 This vulnerability was introduced in v5.1-rc1. After receiving the attached frames, the kernel log looks like that: \_\_\_\_\_\_ BUG: KASAN: use-after-free in cfg80211 inform bss frame data (net/wireless/scan.c:2536) Read of size 8 at addr ffff888008d04478 by task ksoftirgd/1/20 Its patch fixes a root cause for at least four UAFs and other different memory issues, including: BUG: KASAN: use-after-free in cmp bss+0x856/0x920 Read of size 8 at addr ffff88801459a068 by task ksoftirqd/0/14 BUG: KASAN: use-after-free in cfg80211 inform single bss data+0xe08/0xea0 Read of size 8 at addr ffff888016272c40 by task ksoftirqd/0/14 BUG: KASAN: use-after-free in cfg80211 put bss+0x261/0x270 Read of size 8 at addr ffff8880162b4248 by task ksoftirqd/0/14 general protection fault, probably for non-canonical address 0xdffffc0200000005: 0000 [#1] PREEMPT SMP KASAN: probably user-memory-access in range [0x0000001000000028-0x000000100000002f] general protection fault, probably for non-canonical address 0xdffffc000000001: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x00000000000008-0x000000000000] general protection fault, probably for non-canonical address 0xf999959999999a: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: maybe wild-memory-access in range [0xcccccccccccd0-0xcccccccccd7] # CVE-2022-42721 This vulnerability was introduced in v5.1-rc1 and leads to an endless loop, leading to a DoS. This is the related kernel log: watchdog: BUG: soft lockup - CPU#0 stuck for 52s! [ksoftirgd/0:14] # CVE-2022-42722 For this, a P2P device is required. This is e.g. default behavior when running NetworkManager to the best of my knowledge. If there is no P2P device yet, it must be created for the reproduction: ip 1 set wlan0 up iw wlan0 interface add p2p0 type \_\_p2pdev addr 02:00:00:00:00:00 iw wdev 0x2 p2p start

general protection fault, probably for non-canonical address 0xdffffc0000000064: 0000 [#1] PREEMPT SMP

Running the PoC leads to a null-ptr-dereference and thus to a DoS:

```
KASAN PTT
KASAN: null-ptr-deref in range [0x00000000000320-0x0000000000327]
For more details, please see the full logs for each CVE attached.
Best
Sönke from SEEMOO @ TU Darmstadt
View attachment "CVE-2022-41674-decoded.log" of type "text/x-log" (5387 bytes)
View attachment "CVE-2022-42719-decoded.log" of type "text/x-log" (7840 bytes)
View attachment "CVE-2022-42720-decoded.log" of type "text/x-log" (8413 bytes)
View attachment "CVE-2022-42721-decoded.log" of type "text/x-log" (7153 bytes)
View attachment "CVE-2022-42722-decoded.log" of type "text/x-log" (7813 bytes)
```

Download attachment "CVE-2022-41674.pcap" of type "application/vnd.tcpdump.pcap" (1110 bytes)

Download attachment "CVE-2022-42720.pcap" of type "application/vnd.tcpdump.pcap" (1472 bytes)

Download attachment "CVE-2022-42721.pcap" of type "application/vnd.tcpdump.pcap" (1472 bytes)

Download attachment "CVE-2022-42722.pcap" of type "application/vnd.tcpdump.pcap" (94 bytes)

Powered by blists - more mailing lists

Please check out the Open Source Software Security Wiki, which is counterpart to this mailing list.

Confused about mailing lists and their use? Read about mailing lists on Wikipedia and check out these guidelines on proper formatting of your messages.

