```
Date: Wed, 15 Sep 2021 14:54:43 +0800
From: "Luo Likang" <luolikang@...ocus.com>
To: <oss-security@...ts.openwall.com>
Subject: CVE-2021-3752: Linux kernel: a uaf bug in bluetooth

A uaf vulnerability in the linux kernel Bluetooth module.

# Analyse

## l2cap_sock_alloc

l2cap_sock_alloc will create a sock and chan object,
sk->chan = chan;
chan->data = sock;

##l2cap_sock_release

static int l2cap_sock_release(struct socket *sock) {
       struct sock *sk = sock->sk;
……
       bt_sock_unlink(&l2cap_sk_list, sk);
       ……
       sock_orphan(sk);
       l2cap_sock_kill(sk); // if sock_zapped in sock->flags and
sk->refcnt-1 == 0 ,it will free the sk object ……
       l2cap_chan_put(chan);// if chan->kref -1 == 0, it will free the chan
obj
       ……
}
So if sk->skc_refcnt=1,sk->flags&sock_zapped >= 1, and chan->kref=2, then sk
will be freed,
but chan will not be freed, chan->data is not set to NULL, which means chan
still retains sk's pointer and will trigger uaf .

So we need to find how to increase chan->kref and set sk->flags=SOCK_ZAPPED

## l2cap_sock_connect
This func will increase the chan->kref
l2cap_sock_connect
       |->l2cap_chan_connect
              |->__l2cap_chan_add
                     |->l2cap_chan_hold => increase chan->kref

## l2cap_sock_shutdown

l2cap_sock_shutdown
       |->l2cap_chan_close : if chan->state == BT_OPEN
       |-> l2cap_sock_teardown_cb
             |-> sock_set_flag(sk, SOCK_ZAPPED)

# CRASH LOG
The latest version of the kernel and ubuntu20/21 can trigger this
vulnerability, (I have not tested on other linux kernel distributions)

[621459.431656] refcount_t: underflow; use-after-free.
[621459.432963] WARNING: CPU: 5 PID: 29819 at lib/refcount.c:28
refcount_warn_saturate+0xae/0xf0 [621459.434028] Modules linked in: ……
[621459.434087] CPU: 5 PID: 29819 Comm: kworker/5:1 Not tainted
5.11.0-27-generic #29~20.04.1-Ubuntu [621459.434480] Hardware name: VMware,
Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00
02/27/2020 [621459.434538] Workqueue: events l2cap_chan_timeout [bluetooth]
[621459.436472] RIP: 0010:refcount_warn_saturate+0xae/0xf0
[621459.436480] Code: a8 27 38 01 01 e8 67 21 60 00 0f 0b 5d c3 80 3d 95 27
38 01 00 75 91 48 c7 c7 18 23 40 ac c6 05 85 27 38 01 01 e8 47 21 60 00 <0f>
0b 5d c3 80 3d 73 27 38 01 00 0f 85 6d ff ff ff 48 c7 c7 70 23
[621459.436482]
RSP: 0018:ffffa38c8416bdf8 EFLAGS: 00010282 [621459.436909] RAX:
0000000000000000 RBX: ffff8f098fe08910
RCX: 0000000000000027 [621459.436911] RDX: 0000000000000027 RSI:
00000000ffff7fff RDI: ffff8f09b9f58ac8
[621459.436912] RBP: ffffa38c8416bdf8 R08: ffff8f09b9f58ac0 R09:
ffffa38c8416bbb8
[621459.436913] R10: 0000000000000001 R11: 0000000000000001 R12:
ffff8f098fe0bc00
[621459.436914] R13: ffff8f098fe08800 R14: ffff8f098fe08af8 R15:
ffff8f09b9f6bc40
[621459.436915] FS:  0000000000000000(0000) GS:ffff8f09b9f40000(0000)
knlGS:0000000000000000
[621459.436916] CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
[621459.436917] CR2: 00007f44474b1290 CR3: 000000008c010001 CR4:
00000000003706e0
[621459.436937] Call Trace:
[621459.436940]  l2cap_sock_kill.part.0+0x94/0xa0 [bluetooth]
[621459.436970]  l2cap_sock_close_cb+0x29/0x30 [bluetooth]
[621459.436992]  l2cap_chan_timeout+0x8e/0xf0 [bluetooth]
[621459.437013]  process_one_work+0x220/0x3c0
[621459.440820]  worker_thread+0x4d/0x3f0
[621459.440824]  kthread+0x114/0x150
[621459.440863]  ? process_one_work+0x3c0/0x3c0
[621459.440865]  ? kthread_park+0x90/0x90
[621459.440867]  ret_from_fork+0x22/0x30
[621459.440872] ---[ end trace c336fca232c893f5 ]---

#CVE
CVE-2021-3752 is assigned by Redhat

#CREDIT
Likang Luo @NSFOCUS Security Team
```