



index : kernel/git/bluetooth/bluetooth-next.git

master

switch

Bluetooth kernel development tree

Bluetooth group

[about](#) [summary](#) [refs](#) [log](#) [tree](#) [commit](#) [diff](#) [stats](#)

log msg

search

author Zhengchao Shao <shaozhengchao@huawei.com> 2022-10-17 15:58:13 +0800
committer Luiz Augusto von Dentz <luiz.von.dentz@intel.com> 2022-10-17 13:24:30 -0700
commit 42cf46dea905a80f6de218e837ba4d4cc33d6979 (patch)
tree e77e77c096ae8de56b4d896b47c6b71466ccf9f7
parent 9fe208c7117dd3d00a13d1a54aad108e2af6ad17 (diff)
download bluetooth-next-42cf46dea905a80f6de218e837ba4d4cc33d6979.tar.gz

diff options

context: 3

space: include

mode: unified

Bluetooth: L2CAP: fix use-after-free in l2cap_conn_del()

When `l2cap_rcv_frame()` is invoked to receive data, and the `cid` is `L2CAP_CID_A2MP`, if the channel does not exist, it will create a channel. However, after a channel is created, the hold operation of the channel is not performed. In this case, the value of channel reference counting is 1. As a result, after `hci_error_reset()` is triggered, `l2cap_conn_del()` invokes the close hook function of A2MP to release the channel. Then `l2cap_chan_unlock(chan)` will trigger UAF issue.

The process is as follows:

Receive data:

```
l2cap_data_channel()
  a2mp_channel_create() --->channel ref is 2
  l2cap_chan_put() --->channel ref is 1
```

Trigger event:

```
hci_error_reset()
  hci_dev_do_close()
  ...
  l2cap_disconn_cfm()
    l2cap_conn_del()
      l2cap_chan_hold() --->channel ref is 2
      l2cap_chan_del() --->channel ref is 1
      a2mp_chan_close_cb() --->channel ref is 0, release channel
      l2cap_chan_unlock() --->UAF of channel
```

The detailed Call Trace is as follows:

```
BUG: KASAN: use-after-free in __mutex_unlock_slowpath+0xa6/0x5e0
Read of size 8 at addr ffff8880160664b8 by task kworker/u11:1/7593
Workqueue: hci0 hci_error_reset
Call Trace:
```

```
<TASK>
dump_stack_lvl+0xcd/0x134
print_report.cold+0x2ba/0x719
kasan_report+0xb1/0x1e0
kasan_check_range+0x140/0x190
__mutex_unlock_slowpath+0xa6/0x5e0
l2cap_conn_del+0x404/0x7b0
l2cap_disconn_cfm+0x8c/0xc0
hci_conn_hash_flush+0x11f/0x260
hci_dev_close_sync+0x5f5/0x11f0
hci_dev_do_close+0x2d/0x70
hci_error_reset+0x9e/0x140
process_one_work+0x98a/0x1620
worker_thread+0x665/0x1080
kthread+0x2e4/0x3a0
ret_from_fork+0x1f/0x30
</TASK>
```

Allocated by task 7593:

```
kasan_save_stack+0x1e/0x40
__kasan_kmalloc+0xa9/0xd0
l2cap_chan_create+0x40/0x930
amp_mgr_create+0x96/0x990
a2mp_channel_create+0x7d/0x150
l2cap_rcv_frame+0x51b8/0x9a70
l2cap_rcv_acldata+0xaa3/0xc00
hci_rx_work+0x702/0x1220
process_one_work+0x98a/0x1620
worker_thread+0x665/0x1080
kthread+0x2e4/0x3a0
ret_from_fork+0x1f/0x30
```

```
Freed by task 7593:
kasan_save_stack+0x1e/0x40
kasan_set_track+0x21/0x30
kasan_set_free_info+0x20/0x30
___kasan_slab_free+0x167/0x1c0
slab_free_freelist_hook+0x89/0x1c0
kfree+0xe2/0x580
l2cap_chan_put+0x22a/0x2d0
l2cap_conn_del+0x3fc/0x7b0
l2cap_disconn_cfm+0x8c/0xc0
hci_conn_hash_flush+0x11f/0x260
hci_dev_close_sync+0x5f5/0x11f0
hci_dev_do_close+0x2d/0x70
hci_error_reset+0x9e/0x140
process_one_work+0x98a/0x1620
worker_thread+0x665/0x1080
kthread+0x2e4/0x3a0
ret_from_fork+0x1f/0x30
```

```
Last potentially related work creation:
kasan_save_stack+0x1e/0x40
__kasan_record_aux_stack+0xbe/0xd0
call_rcu+0x99/0x740
netlink_release+0xe6a/0x1cf0
__sock_release+0xcd/0x280
sock_close+0x18/0x20
__fput+0x27c/0xa90
task_work_run+0xdd/0x1a0
exit_to_user_mode_prepare+0x23c/0x250
syscall_exit_to_user_mode+0x19/0x50
do_syscall_64+0x42/0x80
entry_SYSCALL_64_after_hwframe+0x63/0xcd
```

```
Second to last potentially related work creation:
kasan_save_stack+0x1e/0x40
__kasan_record_aux_stack+0xbe/0xd0
call_rcu+0x99/0x740
netlink_release+0xe6a/0x1cf0
__sock_release+0xcd/0x280
sock_close+0x18/0x20
__fput+0x27c/0xa90
task_work_run+0xdd/0x1a0
exit_to_user_mode_prepare+0x23c/0x250
syscall_exit_to_user_mode+0x19/0x50
do_syscall_64+0x42/0x80
entry_SYSCALL_64_after_hwframe+0x63/0xcd
```

Fixes: d0be8347c623 ("Bluetooth: L2CAP: Fix use-after-free caused by l2cap_chan_put")
Signed-off-by: Zhengchao Shao <shaozhengchao@huawei.com>
Signed-off-by: Luiz Augusto von Dentz <luiz.von.dentz@intel.com>

Diffstat

```
-rw-r--r-- net/bluetooth/l2cap_core.c 1
```

1 files changed, 1 insertions, 0 deletions

```
diff --git a/net/bluetooth/l2cap_core.c b/net/bluetooth/l2cap_core.c
index 2283871d3f013..9a32ce6349194 100644
--- a/net/bluetooth/l2cap_core.c
+++ b/net/bluetooth/l2cap_core.c
@@ -7615,6 +7615,7 @@ static void l2cap_data_channel(struct l2cap_conn *conn, u16 cid,
     return;
 }

+    l2cap_chan_hold(chan);
+    l2cap_chan_lock(chan);
 } else {
     BT_DBG("unknown cid 0x%4.4x", cid);
```