Disconnecting L2CAP channel right after invalid ATT request leads freeze

Moderate d3zd3z published GHSA-7g38-3x9v-v7vp on Jun 21, 2021

Package **zephyr** (west)	
Affected versions 2.4.0, 2.5.0	Patched versions 2.6.0

Description

Impact

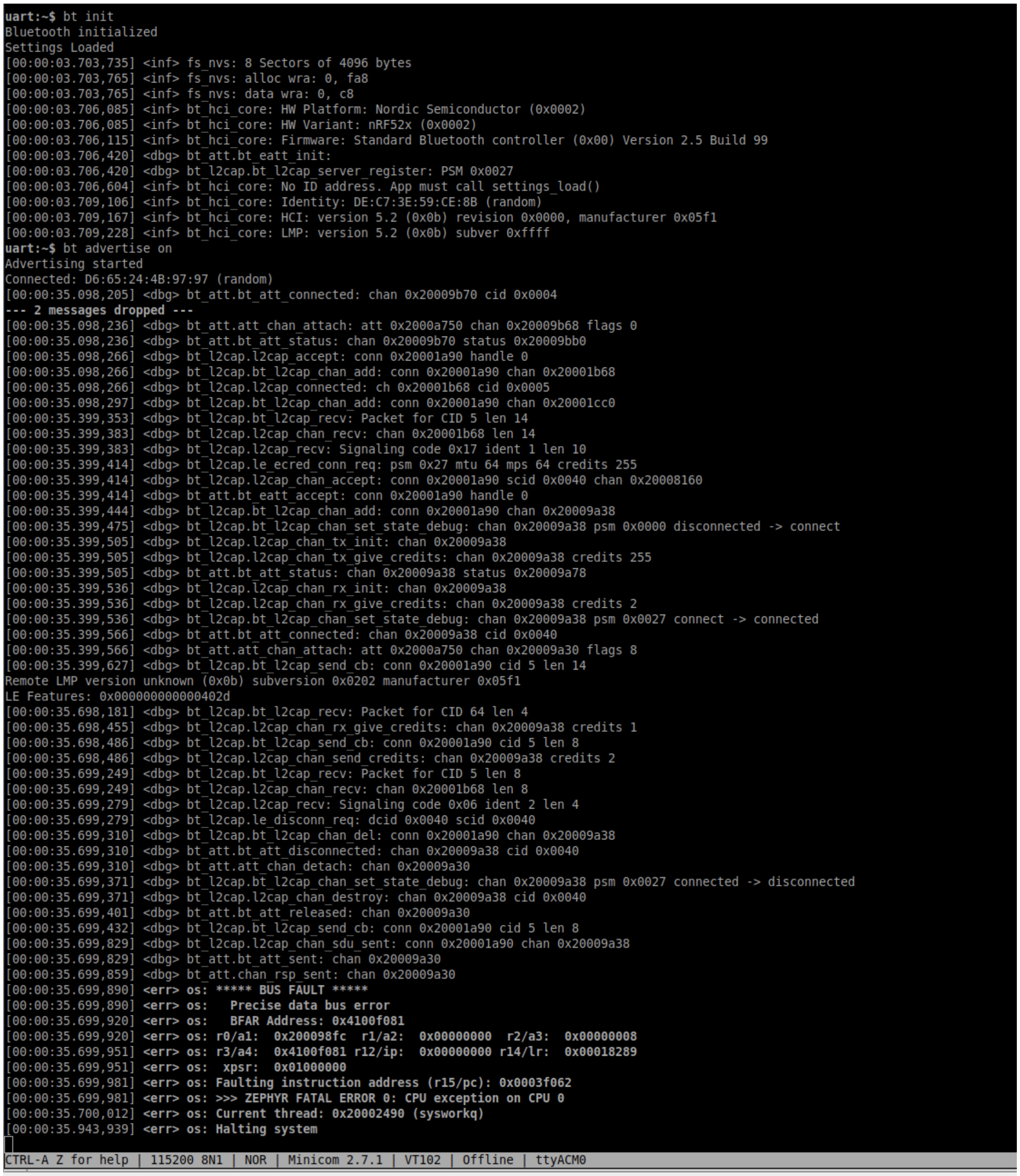
When Central device connects to peripheral and creates L2CAP connection for Enhanced ATT, sending some invalid ATT request and disconnecting immediately causes freeze.

Analysis

Sending malformed ATT request on EATT channel and disconnecting L2CAP immediately crashes the Zephyr. It seems that L2CAP channel is already in disconnected state when Zephyr stack calls sent callback `l2cap_chan_sdu_sent()` and further `bt_att_sent()` . In `bt_att_sent()`

crash happens because already freed memory block is being accessed.

From the logs we can see that `bt_att_disconnected()` and `bt_att_released()` were called which means that memory regions both att channel and att contexts were freed. For some reason Zephyr master does not dump the bus fault message but just silently freezes. Following screenshot is from v2.5-branch.



```
uart:~$ bt init
Bluetooth initialized
Settings Loaded
[00:00:03.703,735] <inf> fs_nvs: 8 Sectors of 4096 bytes
[00:00:03.703,765] <inf> fs_nvs: alloc wra: 0, fa8
[00:00:03.703,765] <inf> fs_nvs: data wra: 0, c8
[00:00:03.706,085] <inf> bt_hci_core: HW Platform: Nordic Semiconductor (0x0002)
[00:00:03.706,085] <inf> bt_hci_core: HW Variant: nRF52x (0x0002)
[00:00:03.706,115] <inf> bt_hci_core: Firmware: Standard Bluetooth controller (0x00) Version 2.5 Build 99
[00:00:03.706,420] <dbg> bt_att.bt_eatt_init:
[00:00:03.706,420] <dbg> bt_l2cap.bt_l2cap_server_register: PSM 0x0027
[00:00:03.706,604] <inf> bt_hci_core: No ID address. App must call settings_load()
[00:00:03.709,106] <inf> bt_hci_core: Identity: DE:C7:3E:59:CE:8B (random)
[00:00:03.709,167] <inf> bt_hci_core: HCI: version 5.2 (0x0b) revision 0x0000, manufacturer 0x05f1
[00:00:03.709,228] <inf> bt_hci_core: LMP: version 5.2 (0x0b) subver 0xffff
uart:~$ bt advertise on
Advertising started
Connected: D6:65:24:4B:97:97 (random)
[00:00:35.098,205] <dbg> bt_att.bt_att_connected: chan 0x20009b70 cid 0x0004
--- 2 messages dropped ---
[00:00:35.098,236] <dbg> bt_att.att_chan_attach: att 0x2000a750 chan 0x20009b68 flags 0
[00:00:35.098,236] <dbg> bt_att.bt_att_status: chan 0x20009b70 status 0x20009bb0
[00:00:35.098,266] <dbg> bt_l2cap.l2cap_accept: conn 0x20001a90 handle 0
[00:00:35.098,266] <dbg> bt_l2cap.bt_l2cap_chan_add: conn 0x20001a90 chan 0x20001b68
[00:00:35.098,266] <dbg> bt_l2cap.l2cap_connected: ch 0x20001b68 cid 0x0005
[00:00:35.098,297] <dbg> bt_l2cap.bt_l2cap_chan_add: conn 0x20001a90 chan 0x20001cc0
[00:00:35.399,353] <dbg> bt_l2cap.bt_l2cap_recv: Packet for CID 5 len 14
[00:00:35.399,383] <dbg> bt_l2cap.l2cap_chan_recv: chan 0x20001b68 len 14
[00:00:35.399,383] <dbg> bt_l2cap.l2cap_recv: Signaling code 0x17 ident 1 len 10
[00:00:35.399,414] <dbg> bt_l2cap.le_ecred_conn_req: psm 0x27 mtu 64 mps 64 credits 255
[00:00:35.399,414] <dbg> bt_l2cap.l2cap_chan_accept: conn 0x20001a90 scid 0x0040 chan 0x20008160
[00:00:35.399,414] <dbg> bt_att.bt_eatt_accept: conn 0x20001a90 handle 0
[00:00:35.399,444] <dbg> bt_l2cap.bt_l2cap_chan_add: conn 0x20001a90 chan 0x20009a38
[00:00:35.399,475] <dbg> bt_l2cap.bt_l2cap_chan_set_state_debug: chan 0x20009a38 psm 0x0000 disconnected -> connect
[00:00:35.399,505] <dbg> bt_l2cap.l2cap_chan_tx_init: chan 0x20009a38
[00:00:35.399,505] <dbg> bt_l2cap.l2cap_chan_tx_give_credits: chan 0x20009a38 credits 255
[00:00:35.399,505] <dbg> bt_att.bt_att_status: chan 0x20009a38 status 0x20009a78
[00:00:35.399,536] <dbg> bt_l2cap.l2cap_chan_rx_init: chan 0x20009a38
[00:00:35.399,536] <dbg> bt_l2cap.l2cap_chan_rx_give_credits: chan 0x20009a38 credits 2
[00:00:35.399,536] <dbg> bt_l2cap.bt_l2cap_chan_set_state_debug: chan 0x20009a38 psm 0x0027 connect -> connected
[00:00:35.399,566] <dbg> bt_att.bt_att_connected: chan 0x20009a38 cid 0x0040
[00:00:35.399,566] <dbg> bt_att.att_chan_attach: att 0x2000a750 chan 0x20009a30 flags 8
[00:00:35.399,627] <dbg> bt_l2cap.bt_l2cap_send_cb: conn 0x20001a90 cid 5 len 14
Remote LMP version unknown (0x0b) subversion 0x0202 manufacturer 0x05f1
LE Features: 0x000000000000402d
[00:00:35.698,181] <dbg> bt_l2cap.bt_l2cap_recv: Packet for CID 64 len 4
[00:00:35.698,455] <dbg> bt_l2cap.l2cap_chan_rx_give_credits: chan 0x20009a38 credits 1
[00:00:35.698,486] <dbg> bt_l2cap.bt_l2cap_send_cb: conn 0x20001a90 cid 5 len 8
[00:00:35.698,486] <dbg> bt_l2cap.l2cap_chan_send_credits: chan 0x20009a38 credits 2
[00:00:35.699,249] <dbg> bt_l2cap.bt_l2cap_recv: Packet for CID 5 len 8
[00:00:35.699,249] <dbg> bt_l2cap.l2cap_chan_recv: chan 0x20001b68 len 8
[00:00:35.699,279] <dbg> bt_l2cap.l2cap_recv: Signaling code 0x06 ident 2 len 4
[00:00:35.699,279] <dbg> bt_l2cap.le_disconn_req: dcid 0x0040 scid 0x0040
[00:00:35.699,310] <dbg> bt_l2cap.bt_l2cap_chan_del: conn 0x20001a90 chan 0x20009a38
[00:00:35.699,310] <dbg> bt_att.bt_att_disconnected: chan 0x20009a38 cid 0x0040
[00:00:35.699,310] <dbg> bt_att.att_chan_detach: chan 0x20009a30
[00:00:35.699,371] <dbg> bt_l2cap.bt_l2cap_chan_set_state_debug: chan 0x20009a38 psm 0x0027 connected -> disconnected
[00:00:35.699,371] <dbg> bt_l2cap.l2cap_chan_destroy: chan 0x20009a38 cid 0x0040
[00:00:35.699,401] <dbg> bt_att.bt_att_released: chan 0x20009a30
[00:00:35.699,432] <dbg> bt_l2cap.bt_l2cap_send_cb: conn 0x20001a90 cid 5 len 8
[00:00:35.699,829] <dbg> bt_l2cap.l2cap_chan_sdu_sent: conn 0x20001a90 chan 0x20009a38
[00:00:35.699,829] <dbg> bt_att.bt_att_sent: chan 0x20009a30
[00:00:35.699,859] <dbg> bt_att.chan_rsp_sent: chan 0x20009a30
[00:00:35.699,890] <err> os: ***** BUS FAULT *****
[00:00:35.699,890] <err> os:   Precise data bus error
[00:00:35.699,920] <err> os:   BFAR Address: 0x4100f081
[00:00:35.699,920] <err> os: r0/a1:  0x200098fc  r1/a2:  0x00000000  r2/a3:  0x00000008
[00:00:35.699,951] <err> os: r3/a4:  0x4100f081 r12/ip:  0x00000000 r14/lr:  0x00018289
[00:00:35.699,951] <err> os:  xpsr:  0x01000000
[00:00:35.699,981] <err> os: Faulting instruction address (r15/pc): 0x0003f062
[00:00:35.699,981] <err> os: >>> ZEPHYR FATAL ERROR 0: CPU exception on CPU 0
[00:00:35.700,012] <err> os: Current thread: 0x20002490 (sysworkq)
[00:00:35.943,939] <err> os: Halting system

CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.7.1 | VT102 | Offline | ttyACM0
```

Patches

This has been fixed in:

- main: #35597
- v2.4: #36105
- v2.5: #36104
- v1.14: TBD

For more information

If you have any questions or comments about this advisory:

- Open an issue in zephyr
- Email us at Zephyr-vulnerabilities

created: 2021-03-19
embargo: 2021-06-19

Severity

Moderate 4.3 / 10

CVSS base metrics

Attack vector	Adjacent
Attack complexity	Low
Privileges required	None
User interaction	None

Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	Low

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVE ID

CVE-2021-3455

Weaknesses

CWE-416

Credits

crd-synopsys

mkarhumaa