zephyrproject-rtos / **zephyr** Public

Code Issues 1.4k Pull requests 523 Discussions Actions ···

Out-of-bound write vulnerability in the Bluetooth mesh core stack can be triggered during provisioning

High **ceolin** published **GHSA-j7v7-w73r-mm5x** on Jul 25

Package

zephyr (west)

Affected versions	Patched versions
<= 3.0	None

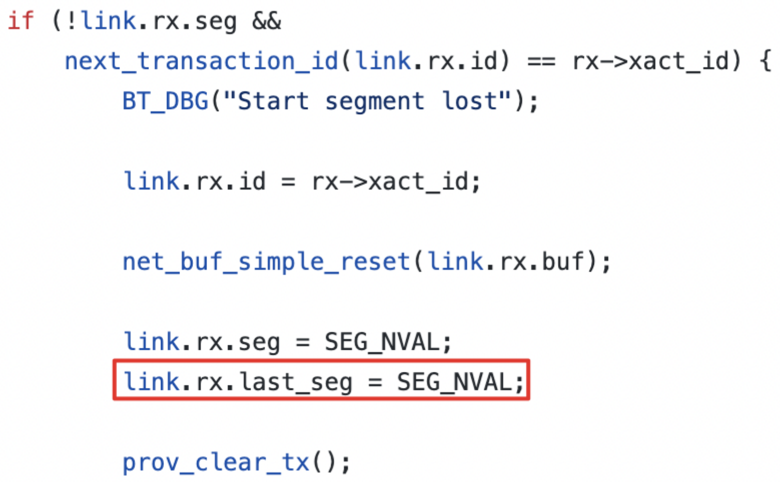
Description

Impact

What kind of vulnerability is it? Who is impacted?

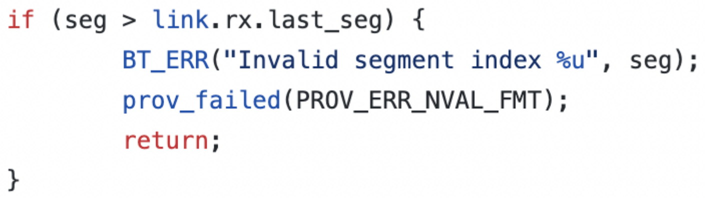
In Zephyr bluetooth mesh core stack, an out-of-bound write vulnerability can be triggered during provisioning. If Transaction Continue PDU is received before the Transaction Start PDU (i.e., start segment lost), the SegN will be initialized as 0xff, which allows subsequent SegO up to 63 and leads to out-of-bound write.

Consider a situation that a Transaction Continue PDU is received first, with SegO greater than 2. SegN (link.rx.last_seg) will be temporarily set as 0xff (SEG_NVAL).



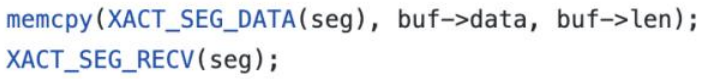
```
if (!link.rx.seg &&
    next_transaction_id(link.rx.id) == rx->xact_id) {
        BT_DBG("Start segment lost");

        link.rx.id = rx->xact_id;

        net_buf_simple_reset(link.rx.buf);

        link.rx.seg = SEG_NVAL;
        link.rx.last_seg = SEG_NVAL;

        prov_clear_tx();
```

Since SegN is 0xff now, we can pass the check SegO <= SegN.



```
if (seg > link.rx.last_seg) {
        BT_ERR("Invalid segment index %u", seg);
        prov_failed(PROV_ERR_NVAL_FMT);
        return;
}
```

Then comes to the memcpy. Since SegO is greater than 2, XACT_SEG_DATA(seg) is greater than 20 + (2-1)×23 = 43, data will be copied beyond 43 + 23 = 66, which exceeds the size of rx_buf, causing out-of-bound write.



```
memcpy(XACT_SEG_DATA(seg), buf->data, buf->len);
XACT_SEG_RECV(seg);
```

```
#define XACT_SEG_DATA(_seg) (&link.rx.buf->data[20 + ((_seg - 1) * 23)])
```

Credits

Han Yan(闫晗),Lewei Qu(曲乐炜),Dongxiang Ke(柯懂湘) of Baidu AIoT Security Team

For more information

If you have any questions or comments about this advisory:

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

embargo: 2022-06-19

Patches

This has been fixed in:

- main: #45066
- v3.0: #45135
- v2.7: #45134

Severity

High 8.2 / 10

CVSS base metrics

Attack vector	Adjacent
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	Low
Availability	Low

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

CVE ID

CVE-2022-1042

Weaknesses

CWE-787