Nordic Bluetooth Mesh SDK transport reassemble-heap overflow 2

Thanks for reviewing !

Any question please contact us at jlu2014yanhan@163.com

Vulnerability description

Nordic Semiconductor is a fabless semiconductor company specializing in wireless technology for the IoT.
Official website : https://www.nordicsemi.com/

In Nordic nRF5 SDK for Mesh, a heap overflow vulnerability can be triggered by sending a series of segmented control packets and access packets with the same *SeqAuth*.

The affected SDK is nRF5 SDK for Mesh. https://www.nordicsemi.com/Products/Development-software/nRF5-SDK-for-Mesh/Download?lang=en#infotabs
The affected version is : version <= v5.0.0
The vulnerable function is *trs_seg_packet_in* in *mesh/core/src/transport.c*.

Vulnerability analysis

Analysis
Segments are linked together using *SeqAuth*.

There is a defect that mesh sdk considers control packet and access packet with the same *SeqAuth* derived from *IVindex*, *SeqZero*, *Seq* as linked segmented packet, which causes them to share the same cache memory. However, memory required by control packet is smaller than that of the access packet,

it could lead to a heap overflow when caching access packet in memory allocated for control packet.

POC

First, we send a control packet with *SeqZero* 4096 and *SegN* 4. It makes the mesh sdk allocate a 40 bytes buffer, and starts to cache the segmented packet with the same *SeqAuth*.

Next, we send several access packets with *SeqZero* 4096, *SegN* 4 and *SegO* 1~4. These packets are considered to be linked with the previous control packets, and are cached into the previously allocated buffer. However, the buffer is too small to cache them all, a heap overflow will then occur.

We added log print before *mesh_mem_alloc* in the *sar_ctx_alloc* and *memcpy* in the *trs_seg_packet_in*. The log demonstrates that allocated buffer size is 40, while the segment offset can be greater than 40, causing heap overflow.

SEGGER Debugger shows the memory state of heap overflow.

Notice that maximum value of *SegN* is 31, corresponding to the overflow size 128 bytes. we just take *SegN* = 4 as an example.

References

Bluetooth Mesh : https://www.bluetooth.com/blog/introducing-bluetooth-mesh-networking/
Bluetooth Mesh Profile : https://www.bluetooth.com/specifications/specs/mesh-profile-1-0-1/