Realtek Semiconductor Corp.
No. 2, Innovation Road II,
Hsinchu Science Park, Hsinchu 300, Taiwan
Tel: +886-3-5780211; Fax: +886-3-5776047

Security Advisory

Published on: April 29, 2022

CVE	*CVE-2022-26528*
Title	Realtek Linux/Android Bluetooth Mesh SDK – An Out-of-bound Write Due to SegO > SegN in Mesh Transport Layer
Description	In Realtek Android Bluetooth Mesh SDK, an out-of-bound write vulnerability can be triggered by sending a series of segmented packets with SegO > SegN. SegO is a lower transport layer field that indicates the segment offset number. SegN is a lower transport layer field that indicates the last segment number. When received first segmented packet, Realtek Android Bluetooth Mesh SDK will allocate a buffer to cache the remaining segmented packets. The size of buffer is (SegN + 1) * single_payload_size, where SegN is parsed from the first segmented packet, and single_payload_size is 8 or 12, depending on the type of packet. The mesh SDK then continues to receive the remaining segmented packets, copies them into the allocated buffer, where the destination address of memcpy is: pbuffer + SegO * single_payload_size. The mesh SDK does not check whether SegO <= SegN when caching packets. Since the buffer size is (SegN + 1) * single_payload_size, if SegO > SegN, an out-of-bound write will occur.
Severity	Medium
CVSSv3	Base score 5.3, CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C
Vulnerability Type	Denial of Service
CWE	CWE-120 : Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') The program copies an input buffer to an output buffer without verifying that the size of the input buffer is less than the size of the output buffer, leading to a buffer overflow.
Affected Chipsets	8723DS,8821CS, 8723FS
Affected Software Versions	Older than Mesh SDK v4.17-4.17-20220127

Acknowledgement

The Realtek Production Security Team would like to thank the following people and parties for finding and responsibly reporting security vulnerabilities to improve Realtek production security.

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

# # #