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-2022-26529*
Title	Realtek Linux/Android Bluetooth Mesh SDK – An Out-of-bound Write Due to Inconsistent Message Type 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 control packets and access packets with the same 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 can lead to an out-of-bound write when caching access packet in memory allocated for control packet.
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

# # #

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