REALTEK

**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-2022-25635* |
|---|---|
| **Title** | Realtek Linux/Android Bluetooth Mesh SDK – An Out-of-bound Write Due to Abnormal BLE Advertising Length |
| **Description** | At initial state, SDK allocated just enough buffer for each advertising packet. Attacker broadcast advertising packets with abnormal data length. The data length of packet was larger than maximum length defined in specification. Our device would scan these packets, delivered them to mesh SDK, SDK copied packets into insufficient buffer, and then buffer overflow happen. |
| **Severity** | Medium |
| **CVSSv3** | Base score 5.3,<br>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 |
| **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

# # #