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: September 17, 2025

CVE	***CVE-2025-49604***
Title	AmebaD WLAN driver defragment issue
Description	In the WLAN driver defragment function, lack of validation of the size of fragmented Wi-Fi frames may lead to a heap-based buffer overflow.
Severity	Medium
CVSSv3	AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Vulnerability Type	Heap Buffer Overflow
CWE	CWE-122 Heap-based Buffer Overflow
Affected Chipsets	RTL8721D
Affected Software Versions	1. https://github.com/Ameba-AIoT/ameba-arduino-d before version 3.1.9 2. https://github.com/Ameba-AIoT/ameba-rtos-d before commit c2bfd8216a1cbc19ad2ab5f48f372ecea756d67a

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.

- Xiaobye(@xiaobye_tw) of DEVCORE Research Team
- Reporter 2, Organization 2

# # #