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

Vulnerability Report

November 24, 2021

Realtek Linux/Android Wi-Fi driver – Buffer Overflow Attack may cause a system crash

Title

Buffer overflow attack may cause a system crash or system security issue

Description

In the Wi-Fi specification, the information field of the Wi-Fi packet consists of ID, length, and values. The length of the information field has its own value range. However, the Wi-Fi Linux/Android driver sometimes does not validate the value of the length of the information field before acquiring it, and uses the value of the length field as the parameter to do a memory copy directly. This operation may potentially cause a system crash or weaken system security.

Vulnerability Type

Overflow

Affected Chipsets

RTL8188E, RTL8188F, RTL8188G, RTL8192E, RTL8192F, RTL8723B, RTL8723D, RTL8723F, RTL8821A, RTL8821C, RTL8812A, RTL8812B, RTL8812C

Revision History

Revision	Date	Description
1.0	November 24, 2021	First version

# # #