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

Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>November 24, 2021</td>
<td>First version</td>
</tr>
</tbody>
</table>

Realtek is a trademark of Realtek Semiconductor Corporation. Other trademarks or registered trademarks mentioned in this release are the intellectual property of their respective owners.