

Vulnerability Report**May 23 2025**

Realtek

Wi-Fi Windows USB Driver

Vulnerability Issue Summary

(ZDI-CAN-24786/ ZDI-CAN-25864/ ZDI-CAN-25857 / ZDI-CAN-
26551 / ZDI-CAN-26553

Release Date

2025/05/23

Affected Projects & Versions:

Version predates 2024/12/31

rtwlanu.sys,

Affected Solution:

Wi-Fi 4/5: RTL8811AU

CVE ID

ZDI-CAN-25864 CVE-2025-8298

ZDI-CAN-25857 CVE-2025-8299

ZDI-CAN-26552 CVE-2025-8300

ZDI-CAN-24786 CVE-2025-8301

ZDI-CAN-26553 CVE-2025-8302.

ZDI-CAN-Issues Description:

There are potential buffer overflow risks in a small fraction of DOT11 OID handling.

MSFT provided test program which can exploit such vulnerabilities and causes BSOD.

Malicious local users might utilize similar tools to attack operating systems..

Be advised that normal users may not encounter such scenario

CVSS Score:

7.8 High

Vector

Will update once reporter request CVE ID.

Root Cause:

Some input buffer lengths and counts used in handling DOT11 OIDs are not strictly validated and hence results in these vulnerabilities.

Solution:

Revise the handling of input buffer check logic to prevent such malicious attack.

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. ☐ "Michael M"

Fixed Version:

Wil-Fi 4/5: RTL8811AU

USB: 1030.52.0325.2025~