

Security Advisory Report

Published on: November 18, 2021
Last Updated on: November 18, 2021

CVE ID

CVE-2022-21742

CVSS

CVSS Basic Score: 2.5

CVSS Vector: CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L/E:U/RL:O/RC:O/AR:L

Severity Rating: Low

Title

Unprivileged user can access device, and may lead to system BSOD.

Description

Realtek has been notified of a potential vulnerability in the Realtek USB Driver for Windows, where an unprivileged user can access a device, which may lead to a system BSOD. Realtek has released driver updates to mitigate this potential vulnerability in the v10.04x driver and later. Check the Realtek Driver Download [Site](#) to obtain the latest update for your products. Realtek also decided not to accept Windows Update requests for impacted versions of the driver, and we suggest users take immediate action to update their system with the latest driver.

Vulnerability Type

Buffer Overflow (CWE-120)

Affected Chipsets

Realtek [USB FE/1GbE/2.5GbE](#) NIC Family

Windows 10, 10.28~10.39/ Windows 8, 8.49~8.60/ Windows 7, 7.42~7.53

Revision History

Revision	Date	Description
	Nov 18, 2021	Preliminary

Acknowledgements:

The issue was reported by Mr. Eran Shimony.

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.