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

Vulnerability Report

March 19, 2024

Realtek AP-Router SDK Advisory – Buffer Overflow

(CVE-2023-49073, CVE-2023-48270, CVE-2023-45742, CVE-2023-49595, CVE-2023-45215, CVE-2023-47856, CVE-2023-50239, CVE-2023-50240, CVE-2023-41251, CVE-2023-50243, CVE-2023-50244, CVE-2023-50330, CVE-2023-49867, CVE-2024-21778)

Release Date

2024/03/19

Affected Projects

Realtek AP-Router SDK

Affected Versions

rtl819x-SDK-v2.x Series
rtl819x-SDK-v3.2.x Series
rtl819x-SDK-v3.4.x Series
rtl819x-SDK-v3.4T Series
rtl819x-SDK-v3.4T-CT Series
rtl819x-SDK-v3.6.0 Series

CVE ID

CVE-2023-49073, CVE-2023-48270, CVE-2023-45742, CVE-2023-49595, CVE-2023-45215, CVE-2023-47856, CVE-2023-50239, CVE-2023-50240, CVE-2023-41251, CVE-2023-50243, CVE-2023-50244, CVE-2023-50330, CVE-2023-49867, CVE-2024-21778

Description

On Realtek Jungle SDK-based routers, buffer overflow vulnerabilities exist in the boa. The root cause of these vulnerabilities is using unsafe APIs such as strcpy(), sprintf(), or memcpy() without checking the length of the destination buffer.

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

Base Score

7.2 High

Vector

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Patch

20240118_sdk_jungle_boa_form_string_vulnerable_modify_patch.tar.gz

20240125_Jungle_patch_for_fix_CVE-2024-21778_of_boa.tar.gz