

Vulnerability Report

March 19, 2024

Realtek AP-Router SDK Advisory – CSRF

(CVE-2023-47677)

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

Realtek

CVE ID

CVE-2023-47677

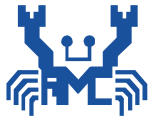
Description

On Realtek Jungle SDK-based routers, the web server's original CSRF protection mechanism only blocks webpage posts if the webpage has not been loaded before. A specially crafted network request from cross-site attackers can bypass this mechanism. A new CSRF protection mechanism can be introduced by verifying a HTTP origin/referrer header and anti-CSRF tokens.

Base Score

8.8 High

Vector



REALTEK

Realtek Semiconductor Corp.

No. 2, Innovation Road II,

Hsinchu Science Park, Hsinchu 300, Taiwan

Tel: +886-3-5780211; Fax: +886-3-5776047

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

Patch

20240319_SDKv3.4T_patch_for_fix_boa_CVE-2023-47677.tar.gz

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.

Realtek