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 – OS Command Injection

(CVE-2023-50381/ CVE-2023-50382/ CVE-2023-50383)

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-2023-50381/ CVE-2023-50382/ CVE-2023-50383

Description

On Realtek Jungle SDK-based routers, three OS command injection vulnerabilities exist in the WPS webpage's handler. The root cause of this is insufficient validation of the received buffer in the webpage's handler and directly taking the received buffer as a parameter of the system's API. To fix these OS command injection vulnerabilities, the handler must validate the input value carefully and filter out illegal characters.

Base Score

7.2 High

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

Vector

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

Patch

20240319_SDKv3.4T_patch_for_fix_boa_CVE-2023-50381~CVE-2023-50383.tar.gz