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

Vulnerability Report

April 21, 2022

Realtek AP-Router SDK Advisory

(CVE-2022-29558)

Release Date

2022/04/21

Affected Projects

Realtek AP-Router Jungle SDK

Affected Versions

rtl819x-SDK-v3.4.x Series

rtl819x-SDK-v3.4T Series

rtl819x-SDK-v3.4T-CT Series

CVE ID

CVE-2022-29558

Description

On Realtek Jungle SDK-based routers, a vulnerability exists in the router's Boa HTTP web server that allows commands injection in the formWlSiteSurvey function. A malicious POST request with a crafted wlanif value could allow a logged in attacker to execute arbitrary commands.

The root cause of the vulnerability is insufficient validation on the receiving buffer. An attack can exploit the vulnerability by crafting arguments in a specific request and execute arbitrary commands.

Vulnerability Type

Improper Input Validation

Attack Type

Network

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

Access Vector

Crafted arguments in a specific request

Security Risk

High

Patch

20220418_sdk_v3.4T-CT_patch_for_fix_attack_of_boa.zip

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.

- Octavio Gianatiempo, Faraday's Security Research team
- Octavio Galland, Faraday's Security Research team
- Emilio Couto, Faraday's Security Research team
- Javier Aguinaga, Faraday's Security Research team