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

Vulnerability Report

August 15, 2021

Realtek AP-Router SDK Advisory

(CVE-2021-35392/CVE-2021-35393/CVE-2021-35394/CVE-2021-35395)

Release Date

2021/08/15

Affected Projects

Realtek AP-Router SDK

Affected Versions

rtl819x-SDK-v3.2.x Series

rtl819x-SDK-v3.4.x Series

rtl819x-SDK-v3.4T Series

rtl819x-SDK-v3.4T-CT Series

rtl819x-eCos-v1.5.x Series

CVE ID

CVE-2021-35392

CVE-2021-35393

CVE-2021-35394

CVE-2021-35395

Description

On some Realtek Jungle SDK based routers, potential memory corruption vulnerabilities in some services may cause their denial of the service.

- **CVE-2021-35392/CVE-2021-35393**

The 'WiFi Simple Config' server (wscd) that implements both UPnP and SSDP protocols is vulnerable to a stack buffer overflow (CVE-2021-35393) due to unsafe parsing of the UPnP SUBSCRIBE/UNSUBSCRIBE Callback header, and also a heap buffer overflow (CVE-2021-35392) due to unsafe crafting of SSDP NOTIFY messages from received M-SEARCH message's ST header.

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

- **CVE-2021-35394**

The 'UDPServer' MP tool is affected by multiple buffer overflow vulnerabilities and an arbitrary command injection vulnerability, due to insufficient legality detection on commands received from clients.

- **CVE-2021-35395**

The HTTP web server 'boa' (go-ahead has been obsoleted) is vulnerable to multiple buffer overflows due to unsafe copies of some overly long parameters submitted in the form, such as

- unsafe copy of 'submit-url' parameter in formRebootCheck/formWsc/formWlanMultipleAP
- unsafe copy of 'ifname' parameter in formWlSiteSurvey
- unsafe copy of 'hostname' parameter in formStaticDHCP
- unsafe copy of 'peerPin' parameter in formWsc

The root cause of the above vulnerabilities is insufficient validation on the received buffer, and unsafe calls to sprintf/strcpy. An attack can exploit the vulnerabilities by crafting arguments in a specific request, and a successful exploit would cause the server to crash and deny service.

Vulnerability Type

Buffer Overflow

Attack Type

Network

Access Vector

Crafting overly long or invalid arguments in a specific request.

Security Risk

High

Patch

- **CVE-2021-35392/CVE-2021-35393/CVE-2021-35394**

20210622_sdk_3.2.3_wsc_binary_and_mp_daemon_patch.tar.gz
20210622_sdk_3.4.11E_wsc_binary_and_mp_daemon_patch.tar.gz
20210705_sdk-v3.4t_pre5_wsc_binary_and_mp_daemon_patch.tar.gz
20210622_sdk-v3.4t_pre7_wsc-upnp-mp.tgz

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

20210701_ecosV1.5.3_patch_for_fixing_vulnerabiits.tar.gz

- **CVE-2021-35395**

20210608_release_v3.2.3_patch_for_fix_buffer_overflow_of_boa.tar.gz

20210608_release_v3.4.11_patch_for_fix_buffer_overflow_of_boa.tar.gz

20210608_release_v3.4T-CT_patch_for_fix_buffer_overflow_of_boa.tar.gz

20210701_ecosV1.5.3_patch_for_fixing_vulnerabiits.tar.gz