Vulnerability Report

March 25, 2022

Realtek AP-Router SDK Advisory

(CVE-2022-27255)

Release Date

2022/03/25

Affected Projects

Realtek AP-Router SDK

Affected Versions

rtl819x-eCos-v0.x Series

rtl819x-eCos-v1.x Series

CVE ID

CVE-2022-27255

Description

On Realtek eCos SDK-based routers, the 'SIP ALG' module is vulnerable to buffer overflow. The root cause of the vulnerability is insufficient validation on the received buffer, and unsafe calls to strcpy. The 'SIP ALG' module calls strcpy to copy some contents of SIP packets to a predefined fixed buffer and does not check the length of the copied contents.

A remote attacker can exploit the vulnerability through a WAN interface by crafting arguments in SDP data or the SIP header to make a specific SIP packet, and the successful exploitation would cause a crash or achieve the remote code execution.

Vulnerability Type

Buffer Overflow

Attack Type

Network

Access Vector

Crafting overly long arguments in a specific SIP packet.

Security Risk

High

Patch

20220314_ecos_fix_crash_caused_by_vulnerability_of_sip_alg.rar

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

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.