EINPRESSWIRE

Remote Code Execution Vulnerability Affects Thousands of Routers Based on Realtek Chipsets

The official presentation of the recently found vulnerability rated 'high severity': CVE 2022-27255

Our research team at #DEFCON30

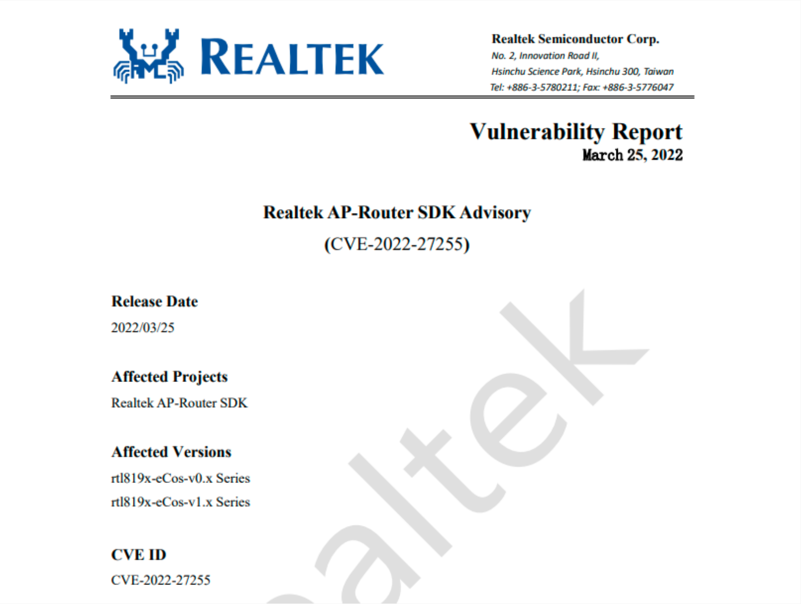
MIAMI, FLORIDA, UNITED STATES, October 5, 2022 /EINPresswire.com/ -- By 2023, the number of devices connected to IP networks will be more than three times the number of people worldwide. Moreover, more people are working from home due to the pandemic. Because of this, the security of a company's network also depends on the security of the home network of its employees. However, most consumer internet-connected devices have a reputation for being vulnerable. This was the starting point for the research team of Faraday Security to seek and report security vulnerabilities in IoT devices, which led to the finding of an exploitable bug in a consumer-grade router popular in Argentina.

> The bottom line of the finding is that, since vendors do not always plan long-term maintenance, security becomes an end user's responsibility."
>
> *Octavio Gianatiempo*

However, the impact of this vulnerability escalated quickly. Researchers Octavio Gianatiempo (@ogianatiempo) and Octavio Galland (@GallandOctavio) presented it at DEFCON 30 in their talk "Exploring the hidden attack surface of OEM IoT devices: pwning thousands of routers with a vulnerability in Realtek's SDK for eCos OS." It was reported and rated 'high severity': CVE 2022-27255

"The vulnerability is a simple buffer overflow that can be triggered remotely without user interaction and under default settings. The vulnerable code is part of the networking stack; if the device is connected to the internet, an attacker only needs to send a packet to take control of the device," said Octavio Gianatiempo when interviewed about the finding.

The vulnerable feature is called SIP ALG. This functionality rewrites SIP messages, a key part of VoIP communications, to ensure that devices on the local network can communicate with devices on the internet. SIP messages can contain SDP data that is used by the parties of the call to establish media sessions. When this implementation of SIP ALG tries to rewrite the media description field in the SDP data of a SIP message, it incurs in a stack buffer overflow by using strcpy without checking the destination buffer size. You can see the advisory here



REALTEK

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 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

RealTek Disclosure

The key part of this finding is that the vulnerability is present in multiple router models from different brands because this particular implementation of SIP ALG is part of a SDK from Realtek. “Realtek SDK for eCos is the code that Realtek provides to vendors who manufacture routers, access points, and repeaters powered by RTL819x family SoCs. This SDK implements the base functionalities of the router, for example, the web administration interface, the networking stack, etc. The vendors can build on top of this SDK to add custom functionalities and their branding to the device.”

“To identify affected products and vendors, our search process combines internet-wide scans, open-source intelligence, and automated firmware analysis. This process is still ongoing, and the number of affected vendors is closer to 20. However, more vendors might be affected that we haven’t found yet. Identifying affected OEM products is daunting due to the lack of visibility of their supply chain. For the moment, most of the identified devices are Tenda, Nexxt, and Intelbras. But there is also a D-Link router affected.” comments Gianatiempo.

A preliminary Shodan search revealed over 60,000 vulnerable routers with their admin panel exposed worldwide. This admin panel is not enabled by default, so the total number of exposed devices should be greater. Remote identification of affected routers without this panel would require triggering the vulnerability, which is outside our research scope.

“Realtek informed customers about the eCos SDK vulnerability in March when it announced the availability of a patch. However, it’s up to the OEMs using the SDK to ensure that the patch is distributed to end-user devices,” writes Eduards Kovacs for SecurityWeek

Up to this date and to the best of our knowledge, no OEM or vendor has released a patched version of their firmware. And since many of these devices do not update automatically, when a patch becomes available, end users would still have to manually update their products. However, if vendors do not patch their firmwares, the best alternative should be to change to a different non-vulnerable product.

The bottom line of the finding is that, since vendors do not always plan long-term maintenance, security becomes an end user’s responsibility. This is why we are publishing the list of affected devices we have found so far alongside our detection tool to identify vulnerable firmware images. We encourage you to try it and help us find other vulnerable products.

Faraday Security
Faraday Security
+1 904-715-4284
socialacc@faradaysec.com
Visit us on social media:
Facebook
Twitter
LinkedIn
Other

This press release can be viewed online at: https://www.einpresswire.com/article/593554414

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2022 Newsmatics Inc. All Right Reserved.