

Unpatched Linux bug may open devices to serious attacks over Wi-Fi



reader comments

25 with 16 posters participating, including story author

Share this story

A potentially serious vulnerability in Linux may make it possible for nearby devices to use Wi-Fi signals to crash or fully compromise vulnerable machines, a security researcher said.

The flaw is located in the RTLWIFI driver, which is used to support Realtek Wi-Fi chips in Linux devices. The vulnerability triggers a buffer overflow in the Linux kernel when a machine with a Realtek Wi-Fi chip is within radio range of a malicious device. At a minimum, exploits would cause an

operating-system crash and could possibly allow a hacker to gain complete control of the computer. The flaw dates back to version 3.10.1 of the Linux kernel released in 2013.

“The bug is serious,” Nico Waisman, who is a principal security engineer at Github, told Ars. “It’s a vulnerability that triggers an overflow remotely through Wi-Fi on the Linux kernel, as long as you’re using the Realtek (RTLWIFI) driver.”

The vulnerability is tracked as CVE-2019-17666. Linux developers proposed a fix on Wednesday that will likely be incorporated into the OS kernel in the coming days or weeks. Only after that will the fix make its way into various Linux distributions.

Waisman said he has not yet devised a proof-of-concept attack that exploits the vulnerability in a way that can execute malicious code on a vulnerable machine.

“I’m still working on exploitation, and it will definitely... take some time (of course, it might not be possible),” he wrote in a direct message. “On paper, [this] is an overflow that should be exploitable. Worst-case scenario, [this] is a denial of service; best scenario, you get a shell.”

After the vulnerability became public, the researcher discussed the flaw on Twitter.

Notice of Absence

The driver flaw can be triggered when an affected device is within radio range of a malicious device. As long as the Wi-Fi is turned on, it requires no interaction on the part of the end user. The malicious device exploits the vulnerability by using a power-saving feature known as a Notice of Absence that’s built into Wi-Fi Direct, a standard that allows two devices to connect over Wi-Fi without the need of an access point. The attack would work by adding vendor-specific

information elements to Wi-Fi beacons that, when received by a vulnerable device, trigger the buffer overflow in the Linux kernel.

The vulnerability only affects Linux devices that use a Realtek chip when Wi-Fi is turned on. The flaw can't be triggered if Wi-Fi is turned off or if the device uses a Wi-Fi chip from a different manufacturer. Based on links [here](#) and [here](#), it appears that Android devices with Realtek Wi-Fi chips may also be affected.

Representatives of both Realtek and Google didn't immediately comment on this story.

While it's still not clear how severely this vulnerability can be exploited, the prospect of code-execution attacks that can be staged wirelessly by devices within radio range is serious. This post will be updated if new information becomes available.

<https://arstechnica.com/?p=1587437>