Chip flaw exposes billions of WiFi devices

February 28 2020, by Peter Grad

Credit: CC0 Public Domain

Billions of WiFi devices were exposed to potential hackers due to a chip vulnerability, security experts said in a report released Wednesday.

Researchers at the cybersecurity firm ESET said they uncovered the problem in chips manufactured by Cypress Semiconductor and

Broadcom. The vulnerability, named KrØØk, affects a wide range of devices including iPhones, Macs, iPads, Amazon Kindles and Echos, as well as Google, Samsung and Raspberry devices. Also affected were WiFi routers by Asus and Huawei.

A hacker would need to be in close proximity to a compromised device to obtain any sensitive data. Even then, only tiny bits of information can be grabbed at a time, although an aggressive attack could potentially yield passwords, user names and other sensitive pieces of information.

Wireless connections using the WPA2 personal and enterprise protocols are affected by KrØØk, as are web connections using the unencrypted HTTP protocol. Mozilla announced earlier this week that it has begun upgrading all Firefox browsers with default DNS over HTTPS, or DoH, domain address retrieval settings, which would protect users from intruders employing weapons such as KrØØk.

The vulnerability exposes user data when a user moves from one WiFi access point to another. When a device disassociates from an access point, it submits unsent data to a buffer that in turn transmits the data with an unsecure key consisting of all zeros. Hackers can transmit their own disassociation frames to exploit the vulnerability and capture data.

ESET researchers, addressing a cybersecurity convention in San Francisco, said that Broadcom and Cypress were notified of the exploits last year and that patches correcting the problems were distributed to device manufacturers.

"According to our information, patches for devices by major manufacturers have been released by now," the researchers said. "To protect yourself, as a user, make sure you have applied the latest available updates to your WiFi-capable devices, including phones, tablets, laptops, IoT devices, and WiFi access points and routers."

Apple and Amazon have confirmed patches were installed on their devices. But researchers cautioned that some devices that don't auto-upgrade, such as WiFi routers, may remain vulnerable. Users should check with device manufacturers if they are unsure of their status.

On ESET's list of affected devices are:

- Amazon Echo 2nd gen
- Amazon Kindle 8th gen
- Apple iPad mini 2
- Apple iPhone 6, 6S, 8, XR
- Apple MacBook Air Retina 13-inch 2018
- Google Nexus 5
- Google Nexus 6
- Google Nexus 6S
- Raspberry Pi 3
- Samsung Galaxy S4 GT-I9505
- Samsung Galaxy S8
- Xiaomi Redmi 3S
- Asus RT-N12
- Huawei B612S-25d
- Huawei EchoLife HG8245H
- Huawei E5577Cs-321

More information: www.rsaconference.com/usa/agen … nerable-wifi-devices