TechXplore

Newly discovered Wi-Fi vulnerabilities called FragAttacks place all mobile devices at risk

May 13 2021, by Sarah Katz

Mobile phone. Credit: Unsplash.com

Fragmentation and aggregation attacks—or frag attacks—refer to a series of design flaws and programming security vulnerabilities affecting Wi-Fi devices. Recent studies have shown that any attacker within radio range of a target can potentially exploit these flaws.

Research indicates that while the design flaws may prove more challenging to abuse due to the need for user interaction or uncommon network settings, the vulnerabilities related to programming pose a more significant risk. Unfortunately, these security flaws affect all contemporary Wi-Fi security protocols, from today's latest WPA3 spanning back to WEP beginning in 1997. This means that a plethora of devices have likely had similar vulnerabilities for many years.

Given the enhanced security protocols for Wi-Fi products over the years, these vulnerabilities have come as something of a surprise. In fact, researchers revealed that the flaws originated with some of the first Wi-Fi protocol back in the mid-1990s. That said, the flaws in programming exist in all mobile devices.

Once an attacker gets into close range of a mobile device user, they can potentially exploit the programming vulnerabilities by inserting plaintext frames into a protected Wi-Fi network. Because certain devices trust plaintext aggregated frames that look like handshake messages, many users could fall victim to such an attack. Hackers could then intercept traffic to the device in question by tricking the target into using an evil DNS server. Research further showed that this vulnerability impacted two of four tested home routers as well as several IoT devices and various smartphones.

Other detected vulnerabilities include how the Wi-Fi standard segments and reassembles network packets, enabling an attacker to extract data by injecting malicious code during this transitionary process.

Thus far, since being notified of these security flaws, the Wi-Fi Alliance has been working with device vendors for the past nine months to mitigate these issues. At this time, Microsoft has addressed three of the

12 bugs affecting Windows systems via patches released on March 9. Next, we should be able to expect a related patch to the Linux kernel.

Furthermore, the Industry Consortium for Advancement of Security (ICASI) on the Internet has reported that the companies Cisco, HPE/Aruba Networks and Sierra Wireless have started developing patches to address the vulnerabilities.

For now, users can check whether their mobile devices have initiated the necessary updates by assessing firmware changelogs for the related CVE listed on ICASI's website. Users who desire an alternative security option can make sure to always visit websites using HTTPS protocol.

More information: FragAttacks: www.fragattacks.com/

Citation: Newly discovered Wi-Fi vulnerabilities called FragAttacks place all mobile devices at risk (2021, May 13) retrieved 26 April 2024 from https://techxplore.com/news/2021-05-newly-wi-fi-vulnerabilities-fragattacks-mobile.html