

New Wi-Fi Attack Allows Traffic Interception, Security Bypass

A group of academic researchers with Northeastern University in Boston and KU Leuven in Belgium have devised a new attack that can intercept Wi-Fi traffic at the MAC (media access control) layer, even between clients that are not allowed to communicate with one another.

The attack exploits a Wi-Fi client isolation bypass vulnerability tracked as CVE-2022-47522 and impacts Wi-Fi networks with malicious insiders, but can also be used to bypass Dynamic ARP inspection (DAI), the academics say in their research paper (PDF).

The attack is based on the idea that, once Wi-Fi clients are connected to a network, packets are routed based on MAC addresses, which allows an attacker to disconnect a victim device and connect under the MAC address of the victim. The attack can only intercept data sent to the victim.

“Any packets that were still underway to the victim, such as website data that the victim was still loading, will now be received by the adversary instead,” the researchers explain.

To set up an attack, an adversary first needs to wait for a client to connect to a vulnerable access point (AP), which is typically followed by a request sent to a server over the internet.

The attacker then needs to forcibly disconnect the victim from the AP before the response arrives, spoof the MAC address of

the victim to connect to the network using the adversary's credentials, and then intercept the response from the server, which the AP will send to the spoofed MAC address.

"We remark that intercepted traffic may be protected by higher-layer encryption, such as TLS and HTTPS. Nevertheless, even if higher-layer encryption is being used, our attack still reveals the IP address that a victim is communicating with. This in turn reveals the websites that a victim is visiting, which can be sensitive information on its own," the researchers note.

The issue, the academics explain, is related to the power-save mechanism that has been part of the IEEE 802.11 standard since the beginning, which can be exploited to leak frames in plaintext, allowing an attacker to force queue frames meant for a specific client, leading to device disconnection, and causing a denial-of-service (DoS) condition.

According to the researchers, "an attacker can override and control the security context of frames that are yet to be queued. This exploits a design flaw in hotspot-like networks and allows the attacker to force an access point to encrypt yet to be queued frames using an adversary-chosen key, thereby bypassing Wi-Fi encryption entirely."

The vulnerability, the academics say, has an impact on a wide range of devices and operating systems, including Linux, FreeBSD, Android, and iOS, which can be exploited to hijack TCP connections or to intercept client and web traffic.

The researchers also released an open source tool called MacStealer, which tests Wi-Fi networks for CVE-2022-47522.

In an advisory this week, Cisco confirmed that its wireless access point products and Meraki products with wireless capabilities are impacted by the vulnerability, noting that the attack is rather opportunistic, only providing an adversary with information "of minimal value in a securely

configured network”.

Related: Passengers Exposed to Hacking via Vulnerabilities in Airplane Wi-Fi Devices

Related: Researchers: Wi-Fi Probe Requests Expose User Data

Related: Researchers Find 226 Vulnerabilities in Nine Wi-Fi Routers

New Wi-Fi Attack Allows Traffic Interception, Security Bypass