[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@4d45bdcf69594a57bc21e2c3bdb8b095?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

ref <https://arstechnica.com/gadgets/2021/05/farewell-to-firewalls-wi-fi-bugs-open-network-devices-to-remote-hacks/>

**Vulnerabilities in billions of Wi-Fi devices let hackers bypass firewalls**

**FragAttacks let hackers inject malicious code or commands into encrypted Wi-Fi traffic.**

[DAN GOODIN](https://arstechnica.com/author/dan-goodin/) - 5/21/2021, 8:39 AM

[Enlarge](https://cdn.arstechnica.net/wp-content/uploads/2021/05/fragattacks.jpg)Mathy Vanhoef[89WITH 59 POSTERS PARTICIPATING](https://arstechnica.com/gadgets/2021/05/farewell-to-firewalls-wi-fi-bugs-open-network-devices-to-remote-hacks/?comments=1)

* [SHARE ON FACEBOOK](https://www.facebook.com/sharer.php?u=https%3A%2F%2Farstechnica.com%2F%3Fpost_type%3Dpost%26p%3D1766544)
* [SHARE ON TWITTER](https://twitter.com/share?text=Vulnerabilities+in+billions+of+Wi-Fi+devices+let+hackers+bypass+firewalls&url=https%3A%2F%2Farstechnica.com%2F%3Fpost_type%3Dpost%26p%3D1766544)

One of the things that makes Wi-Fi work is its ability to break big chunks of data into smaller chunks and combine smaller chunks into bigger chunks, depending on the needs of the network at any given moment. These mundane network plumbing features, it turns out, have been harboring vulnerabilities that can be exploited to send users to malicious websites or exploit or tamper with network-connected devices, newly published research shows.

In all, researcher Mathy Vanhoef found a dozen vulnerabilities, either in the Wi-Fi specification or in the way the specification has been implemented in huge numbers of devices. Vanhoef has dubbed the vulnerabilities [FragAttacks](https://www.fragattacks.com/), short for fragmentation and aggregation attacks, because they all involve frame fragmentation or frame aggregation. Broadly speaking, they allow people within radio range to inject frames of their choice into networks protected by WPA-based encryption.

**Bad news**

**FURTHER READING**

[Serious flaw in WPA2 protocol lets attackers intercept passwords and much more](https://arstechnica.com/information-technology/2017/10/severe-flaw-in-wpa2-protocol-leaves-wi-fi-traffic-open-to-eavesdropping/)Assessing the impact of the vulnerabilities isn’t straightforward. FragAttacks allow data to be injected into Wi-Fi traffic, but they don’t make it possible to exfiltrate anything out. That means FragAttacks can’t be used to read passwords or other sensitive information the way a previous Wi-Fi attack of Vanhoef, called [Krack](https://arstechnica.com/information-technology/2017/10/severe-flaw-in-wpa2-protocol-leaves-wi-fi-traffic-open-to-eavesdropping/), did. But it turns out that the vulnerabilities—some that have been part of Wi-Fi since its release in 1997—can be exploited to inflict other kinds of damage, particularly if paired with other types of hacks.

“It's never good to have someone able to drop packets into your network or target your devices on the network,” Mike Kershaw, a Wi-Fi security expert and developer of the open source Kismet wireless sniffer and IDS, wrote in an email. “In some regards, these are no worse than using an unencrypted access point at a coffee shop—someone can do the same to you there, trivially—but because they can happen on networks you'd otherwise think are secure and might have configured as a trusted network, it's certainly bad news.”

He added: “Overall, I think they give someone who was already targeting an attack against an individual or company a foothold they wouldn't have had before, which is definitely impactful, but probably don’t pose as huge a risk as drive-by attacks to the average person.”

While the flaws were disclosed last week in an industry-wide effort nine months in the making, it remains unclear in many cases which devices were vulnerable to which vulnerabilities and which vulnerabilities, if any, have received security updates. It’s almost a certainty that many Wi-Fi-enabled devices will never be fixed.

**Rogue DNS injection**

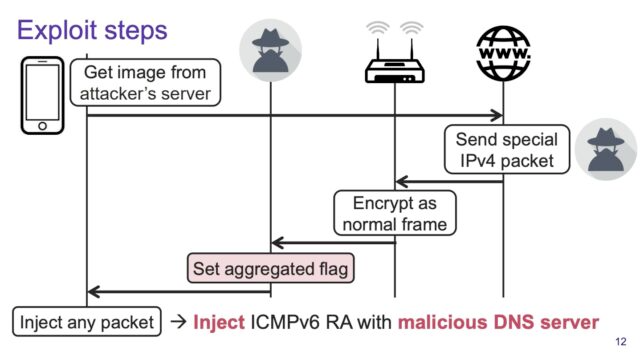
One of the most severe vulnerabilities in the FragAttacks suite resides in the Wi-Fi specification itself. Tracked as CVE-2020-24588, the flaw can be exploited in a way that forces Wi-Fi devices to use a rogue DNS server, which in turn can deliver users to malicious websites rather than the ones they intended. From there, hackers can read and modify any unencrypted traffic. Rogue DNS servers also allow hackers to perform [DNS rebinding attacks](https://danielmiessler.com/blog/dns-rebinding-explained/), in which malicious websites manipulate a browser to attack other devices connected to the same network.

The rogue DNS server is introduced when an attacker injects an [ICMPv6 Router Advertisement](http://www.tcpipguide.com/free/t_ICMPv6RouterAdvertisementandRouterSolicitationMess-2.htm) into Wi-Fi traffic. Routers typically issue these announcements so other devices on the network can locate them. The injected advertisement instructs all devices to use a DNS specified by the attacker for lookups of both IPv6 and IPv4 addresses.

An exploit demoed in a video Vanhoef published shows the attacker luring the target to a website that stashes the router advertisement in an image.

FragAttacks: Demonstration of Flaws in WPA2/3.

Here's a visual overview:

[Enlarge](https://cdn.arstechnica.net/wp-content/uploads/2021/05/dns-injection.jpg)Mathy Vanhoef

In an email, Vanhoef explained, saying, “The IPv6 router advertisement is put in the payload (i.e. data portion) of the TCP packet. This data is by default passed on to the application that created the TCP connection. In the demo, that would be the browser, which is expecting an image. This means that by default, the client won't process the IPv6 router advertisement but instead process the TCP payload as application data.”

Vanhoef said that it’s possible to perform the attack without user interaction when the target’s access point is vulnerable to [CVE-2021-26139](https://nvd.nist.gov/vuln/detail/CVE-2020-26139), one of the 12 vulnerabilities that make up the FragAttacks package. The security flaw stems from a kernel flaw in NetBSD 7.1 that causes Wi-Fi access points to forward [Extensible Authentication Protocol (AP) over LAN](https://en.wikipedia.org/wiki/IEEE_802.1X) frames to other devices even when the sender has not yet authenticated to the AP.

It’s safe to skip ahead, but for those curious about the specific software bug and the reason the video demo uses a malicious image, Vanhoef explained:

To make the victim process the TCP payload (i.e. data portion) as a separate packet, the aggregation design flaw in Wi-Fi is abused. That is, the attacker intercepts the malicious TCP packet at the Wi-Fi layer and sets the "is aggregated" flag in the Wi-Fi header. As a result, the receiver will split the Wi-Fi frame into two network packets. The first network packet contains part of the original TCP header and is discarded. The second packet corresponds with the TCP payload, which we made sure will now correspond to the ICMPv6 packet, and as a result, the ICMPv6 router advertisement is now processed by the victim as a separate packet. So proximity to the victim is required to set the "is aggregated" Wi-Fi flag so that the malicious TCP packet will be split into two by the receiver.

The design flaw is that an adversary can change/set the "is aggregated" flag without the receiver noticing this. This flag should have been authenticated so that a receiver can detect if it has been modified.

It's possible to perform the attack without user interaction when the access point is vulnerable to CVE-2020-26139. Out of four tested home routers, two of them had this vulnerability. It seems that most Linux-based routers are affected by this vulnerability. The research paper discusses in more detail how this works—essentially, instead of including the ICMPV6 router advertisement in a malicious TCP packet, it can then be included in an unencrypted handshake message (which the AP will then forward to the client after which the adversary can again set the "is aggregated" flag etc).

**Punching a hole in the firewall**

Four of the 12 vulnerabilities that make up the FragAttacks are implementation flaws, meaning they stem from bugs that software developers introduced when writing code based on the Wi-Fi specification. An attacker can exploit them against access points to bypass a key security benefit they provide.

Besides allowing multiple devices to share a single Internet connection, routers prevent incoming traffic from reaching connected devices unless the devices have requested it. This firewall works by using network address translation, or NAT, which maps private IP addresses that the AP assigns each device on the local network to a single IP address that the AP uses to send data over the Internet.

The result is that routers forward data to connected devices only when they have previously requested it from a website, email server, or other machine on the Internet. When one of those machines tries to send unsolicited data to a device behind the router, the router automatically discards it. This arrangement [isn’t perfect](https://www.f5.com/services/resources/white-papers/the-myth-of-network-address-translation-as-security), but it does provide a vital defense that protects billions of devices.

Vanhoef figured out how to exploit the four vulnerabilities in a way that allows an attacker to, as he put it, “punch a hole through a router’s firewall.” With the ability to connect directly to devices behind a firewall, an Internet attacker can then send them malicious code or commands.

In one demo in the video, Vanhoef exploits the vulnerabilities to control an Internet-of-things device, specifically to remotely turn on and off a smart power socket. Normally, NAT would prevent a device outside the network from interacting with the socket unless the socket had first initiated a connection. The implementation exploits remove this barrier.

**FURTHER READING**

[Microsoft practically begs Windows users to fix wormable BlueKeep flaw](https://arstechnica.com/information-technology/2019/05/microsoft-says-its-confident-an-exploit-exists-for-wormable-bluekeep-flaw/)In a separate demo, Vanhoef shows how the vulnerabilities allow a device on the Internet to initiate a connection with a computer running Windows 7, an operating system that stopped receiving security updates years ago. The researcher used that ability to gain complete control over the PC by sending it malicious code that exploited a [critical vulnerability called BlueKeep](https://arstechnica.com/information-technology/2019/05/microsoft-says-its-confident-an-exploit-exists-for-wormable-bluekeep-flaw/).

“That means that when an access point is vulnerable, it becomes easy to attack clients!” Vanhoef wrote. “So we're abusing the Wi-Fi implementation flaws in an *access point* as a first step in order to subsequently attack (outdated) *clients*.”

**Getting your fix**

Despite Vanhoef spending nine months coordinating patches with more than a dozen hardware and software makers, it’s not easy to figure out which devices or software are vulnerable to which vulnerabilities, and of those vulnerable products, which ones have received fixes.

[This page](https://www.icasi.org/aggregation-fragmentation-attacks-against-wifi/) provides the status for products from several companies. A more comprehensive list of known advisories is [here](https://github.com/vanhoefm/fragattacks/blob/master/ADVISORIES.md). Other advisories are available individually from their respective vendors. The vulnerabilities to look for are:

**Design flaws:**

* [CVE-2020-24588](https://nvd.nist.gov/vuln/detail/CVE-2020-24588): aggregation attack (accepting non-SPP A-MSDU frames)
* [CVE-2020-24587](https://nvd.nist.gov/vuln/detail/CVE-2020-24587): mixed key attack (reassembling fragments encrypted under different keys)
* [CVE-2020-24586](https://nvd.nist.gov/vuln/detail/CVE-2020-24586): fragment cache attack (not clearing fragments from memory when (re)connecting to a network)

**Implementation vulnerabilities allowing the injection of plaintext frames:**

* [CVE-2020-26145](https://nvd.nist.gov/vuln/detail/CVE-2020-26145): Accepting plaintext broadcast fragments as full frames (in an encrypted network)
* [CVE-2020-26144](https://nvd.nist.gov/vuln/detail/CVE-2020-26144): Accepting plaintext A-MSDU frames that start with an RFC1042 header with EtherType EAPOL (in an encrypted network)
* [CVE-2020-26140](https://nvd.nist.gov/vuln/detail/CVE-2020-26140): Accepting plaintext data frames in a protected network
* [CVE-2020-26143](https://nvd.nist.gov/vuln/detail/CVE-2020-26143): Accepting fragmented plaintext data frames in a protected network

**Other implementation flaws:**

* [CVE-2020-26139](https://nvd.nist.gov/vuln/detail/CVE-2020-26139): Forwarding EAPOL frames even though the sender is not yet authenticated (should only affect APs)
* [CVE-2020-26146](https://nvd.nist.gov/vuln/detail/CVE-2020-26146): Reassembling encrypted fragments with non-consecutive packet numbers
* [CVE-2020-26147](https://nvd.nist.gov/vuln/detail/CVE-2020-26147): Reassembling mixed encrypted/plaintext fragments
* [CVE-2020-26142](https://nvd.nist.gov/vuln/detail/CVE-2020-26142): Processing fragmented frames as full frames
* [CVE-2020-26141](https://nvd.nist.gov/vuln/detail/CVE-2020-26141): Not verifying the TKIP MIC of fragmented frames

The most effective way to mitigate the threat posed by FragAttacks is to install all available updates that fix the vulnerabilities. Users will have to do this on each vulnerable computer, router, or other Internet-of-things device. It’s likely that a huge number of affected devices will never receive a patch.

The next-best mitigation is to ensure that websites are always using HTTPS connections. That’s because the encryption HTTPS provides greatly reduces the damage that can be done when a malicious DNS server directs a victim to a fake website.

Sites that use HTTP Strict Transport Security will always use this protection, but Vanhoef said that only about 20 percent of the web does this. Browser extensions like [HTTPS everywhere](https://en.wikipedia.org/wiki/HTTPS_Everywhere) were already a good idea, and the mitigation they provide against FragAttacks makes them even more worthwhile.

As noted earlier, FragAttacks aren’t likely to be exploited against the vast majority of Wi-Fi users, since the exploits require a high degree of skill as well as proximity—meaning within 100 feet to a half-mile, depending on the equipment used—to the target. The vulnerabilities pose a higher threat to networks used by high-value targets such as retail chains, embassies, or corporate networks where security is key, and then most likely only in concert with other exploits.

When updates become available, by all means install them, but unless you’re in this latter group, remember that drive-by downloads and other more mundane types of attacks will probably pose a bigger threat.