[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@8315170bff1b4545af3b459db4495d31?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view" \l "main)

ref <https://www.theverge.com/2021/5/12/22433134/fragattacks-wi-fi-vulnerabilities-update-security>

**A security researcher found Wi-Fi vulnerabilities that have existed since the beginning**

[11](https://www.theverge.com/2021/5/12/22433134/fragattacks-wi-fi-vulnerabilities-update-security#comments)

The cycle of painful updates begins anew

By [Mitchell Clark](https://www.theverge.com/authors/mitchell-clark)  May 12, 2021, 8:59pm EDT

**Share this story**

* [Share this on Facebook (opens in new window)](https://www.facebook.com/sharer/sharer.php?text=A+security+researcher+found+Wi-Fi+vulnerabilities+that+have+existed+since+the+beginning&u=https%3A%2F%2Fwww.theverge.com%2F2021%2F5%2F12%2F22433134%2Ffragattacks-wi-fi-vulnerabilities-update-security)
* [Share this on Twitter (opens in new window)](https://twitter.com/intent/tweet?counturl=https%3A%2F%2Fwww.theverge.com%2F2021%2F5%2F12%2F22433134%2Ffragattacks-wi-fi-vulnerabilities-update-security&text=A+security+researcher+found+Wi-Fi+vulnerabilities+that+have+existed+since+the+beginning&url=https%3A%2F%2Fwww.theverge.com%2F2021%2F5%2F12%2F22433134%2Ffragattacks-wi-fi-vulnerabilities-update-security&via=Verge)
* [SHAREAll sharing options](https://www.theverge.com/2021/5/12/22433134/fragattacks-wi-fi-vulnerabilities-update-security)

*Illustrator by Alex Castro / The Verge*

The security researcher who discovered [the Krack Wi-Fi vulnerability](https://www.theverge.com/2017/10/16/16484824/krack-wifi-encryption-bug-vulnerability-install-patch) has discovered [a slew of other flaws](https://www.fragattacks.com/) with the wireless protocol most of us use to power our online lives ([via *Gizmodo*](https://gizmodo.com/update-windows-and-lots-of-other-stuff-asap-fragatta-1846878065)). The vulnerabilities relate to how Wi-Fi handles large chunks of data, with some being related to the Wi-Fi standard itself, and some being related to how it’s implemented by device manufacturers.

The researcher, Mathy Vanhoef, calls the collection of vulnerabilities “FragAttacks,” with the name being a mashup of “fragmentation” and “aggregation.” He also says the vulnerabilities could be exploited by hackers, allowing them to intercept sensitive data, or show users fake websites, even if they’re using Wi-Fi networks secured with WPA2 or even WPA3. They could also theoretically exploit other devices on your home network.

There are twelve different attack vectors that fall under the classification, which all work in different ways. One exploits routers accepting plaintext during handshakes, one exploits routers caching data in certain types of networks, etc. If you want to read all the technical details on how exactly they work, you can check [out Vanhoef’s website](https://www.fragattacks.com/).

[According to *The Record*](https://therecord.media/wifi-devices-going-back-to-1997-vulnerable-to-new-frag-attacks/), Vanhoef informed the WiFi Alliance about the vulnerabilities that were baked-in to the way Wi-Fi works so they could be corrected before he disclosed them to the public. Vanhoef says that he’s not aware of the vulnerabilities being exploited in the wild. While he points out in a video that some of the vulnerabilities aren’t particularly easy to exploit, he says others would be “trivial” to take advantage of.

Vanhoef points out that some of the flaws can be exploited on networks using the WEP security protocol, indicating that they’ve been around since Wi-Fi was first implemented in 1997 (though if you’re still using WEP, these attacks should be [the least of your concerns](https://www.theverge.com/2014/8/8/5982701/cat-hacking-hack-wifi-war-kitteh)).

Vanhoef says that the flaws are wide-spread, affecting many devices, meaning that there’s a lot of updating to do.

The thing about updating Wi-Fi infrastructure is that it’s always a pain. For example, before writing this article I went to check if my router had any updates, and realized that I had forgotten my login information (and I suspect I won’t be alone in that experience). There’s also devices that are just plain old, whose manufacturers are either gone or not releasing patches anymore. If you can, though, you should keep an eye on your router manufacturer’s website for any updates that are rolling out, especially if they’re [in the advisory list](https://github.com/vanhoefm/fragattacks/blob/master/ADVISORIES.md).

Some vendors have already released patches for some of their products, including:

* Microsoft
* [Eero](https://blog.eero.com/fragattacks-fragmentation-aggregation-and-attacks-update-available-for-all-eero-customers/)
* [Aruba](https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-011.txt)
* [Cisco](https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-wifi-faf-22epcEWu.html)
* [Ruckus](https://support.ruckuswireless.com/fragattacks-ruckus-technical-support-response-center)
* [Intel](https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00473.html)
* [Juniper](https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11170&cat=SIRT_1&actp=LIST)
* [Lancom](https://www.lancom-systems.com/service-support/instant-help/general-security-information/)
* [Lenovo](https://support.lenovo.com/fr/en/product_security/len-57316)
* [Linux Wireless](https://lore.kernel.org/linux-wireless/20210511180259.159598-1-johannes@sipsolutions.net/)
* [Mist](https://www.mist.com/documentation/mist-security-advisory-fragattacks-and-faq)
* [Netgear](https://kb.netgear.com/000063666/Security-Advisory-for-Fragment-and-Forge-vulnerabilities-on-some-WiFi-capable-devices-PSV-2021-0014-PSV-2021-0080)
* [Samsung](https://security.samsungmobile.com/securityUpdate.smsb)
* [Synology](https://www.synology.com/en-global/security/advisory/Synology_SA_21_20)
* [Zyxel](https://community.zyxel.com/en/discussion/10655/zyxel-security-advisory-for-fragattacks-against-wifi-products)

As for anything else you need to do, [Vanhoef recommends](https://www.fragattacks.com/" \l "notpatched) the usual steps: keep your computers updated, use strong, unique passwords, don’t visit shady sites, and make sure you’re using HTTPS as often as possible. Other than that, it’s mostly being thankful that you’re not in charge of widespread IT infrastructure (my deepest condolences if you, in fact, are).