Published on *Jisc community* (https://community.jisc.ac.uk)

2021-06 Advisory: Fragmentation and Aggregation Attacks (FragAttacks)

Published: 14/06/2021

This advisory applies to all organisations providing a Visited (Wi-Fi) service. Whilst not specifically an eduroam/802.1X related issue, the FragAttacks vulnerabilities highlight the need to keep your Wi-Fi devices patched to ensure that fixes developed by your equipment vendors are applied to your infrastructure. Several vendors have been quick to respond and have released updates; you may have received direct e-mail notification.

It has been widely reported in the Wi-Fi industry media that Mathy Vanhoef of New York University Abu Dhabi recently released results of investigations into newly uncovered security vulnerabilities affecting Wi-Fi devices. The collection of fragmentation and aggregation vulnerabilities in unpatched Wi-Fi equipment has been published on the FragAttack web site https://www.fragattacks.com/ [1] and the paper Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation https://papers.mathyvanhoef.com/usenix2021.pdf [2] is due to be presented at the 30th Usenix Security Symposium on August 11–13 2021.

The FragAttacks vulnerabilities result from original Wi-Fi design flaws dating back many years. The vulnerabilities relate to the way in which 802.11 devices receive, store, and process frames that are transmitted using the 802.11 protocol - so are applicable to all Wi-Fi systems.

The paper explicitly names eduroam and govroam, but it should not be inferred that these services are specifically at risk; eduroam and govroam are high profile, well known services in the university research working environment and have been cited as examples of Wi-Fi ‘hotspots’ despite the fact that neither are captive portal or pre-shared key systems.

The risks, whilst hard for attackers to exploit, are however being taken seriously by the eduroam and govroam support communities, and the Wi-Fi industry as a whole. The response of eduroam at a global level, which we completely endorse, is presented on: https://eduroam.org/fragmentation-and-aggregation-attacks-fragattacks-and-eduroam/ [3]

Whilst the actions proposed are sound precautions, it should be noted that most of the vulnerabilities described in the report require multiple things to happen for any attack to be successful and would be very difficult to exploit. It is reassuring to note that none of the 12 Common Vulnerabilities and Exposures (CVEs) are against the encryption or the cryptography used in securing Wi-Fi - particularly not the 802.1X standard and WPA2/AES on which the security of eduroam services is based.

Summary of advice:

- Ensure that the software patching of your Wi-Fi APs is up to date
- Discontinue the use of older Wi-Fi access points for which security updates are no longer available
- Review your device settings to remove open/unsecured automatically connecting Wi-Fi SSIDs to reduce risks using untrustworthy access points.
- Continue user communication about the mounting personal security and account compromise risks of using unpatched devices - the risks associated with use of vulnerable devices outweigh the benefit of being connected
- Apply your site managed eduroam/govroam profile to all clients. This can be done from the Configuration Assistant Tool (CAT) at https://cat.eduroam.org [4] or for govroam contact help@jisc.ac.uk [5]
- eduroam/govroam site AP operators should review the capability of their Wi-Fi equipment to support 802.11w / PMF (Protected Management Frames) in order to mitigate these types of vulnerabilities.

If you have any concerns or additional advice/experience you would like to share, please get in touch via help@jisc.ac.uk [5]

Source URL: https://community.jisc.ac.uk/library/network-and-technology-service-docs/2021-06-advisory-fragmentation-and-aggregation-attacks

Links
[1] https://www.fragattacks.com/
[2] https://papers.mathyvanhoef.com/usenix2021.pdf
[3] https://eduroam.org/fragmentation-and-aggregation-attacks-fragattacks-and-eduroam/
[4] https://cat.eduroam.org/
[5] mailto:help@jisc.ac.uk