

Advisory: WPA2 Key Reinstallation Attacks vulnerability, KRACK

Released: 24th October 2017

This advisory is relevant to all eduroam(UK) Home (IdP) and Visited (SP) service organisations. It's aim is to bring to the attention of our community the vulnerability of WPA2 to Key Reinstallation Attacks (KRACK) and describes the position of eduroam.org together with recommend actions to be taken.

Background and scope:

The WPA2 Key Reinstallation Attacks vulnerability, KRACK was discovered by the Belgian researchers Mathy Vanhoef and Frank Piessens of the University of Leuven and first publicised on 16th October, gathering much media/internet attention. Whilst this is Wi-Fi issue and not core eduroam, since we mandate use of WPA2 for eduroam Wi-Fi, a statement on the vulnerability is appropriate.

The eduroam.org position is described here <https://www.eduroam.org/2017/10/18/key-reinstallation-attack-and-wpa2/> ^[1] and the discoverer of the vulnerability has described it in detail on <https://www.krackattacks.com/> ^[2]

Summary:

An attacker within range of a victim can exploit weaknesses using key reinstallation attacks (KRACKs). The attack is that a temporal encryption key (essentially a bitstream meant to work as a one-time pad) which is meant to be used only once (a per-packet key) is forced to be used more than once. This can lead to the attacker being able to read information that was previously assumed to be safely encrypted. Sensitive information such as credit card numbers, passwords, chat messages, e-mails, photos, etc can be stolen. Depending on the network configuration, it is also possible to inject and manipulate data, resulting in for example, injection of ransomware or other malware into websites. Although websites or apps may use HTTPS as an additional layer of protection, it is warned that this extra protection can still be bypassed in a worrying number of situations including in Apple's iOS and OS X, in Android apps and even in VPN apps. The attack is directional, meaning that the direction, client to AP / AP to client, in which packets can be decrypted (and possibly forged) depends on the handshake being attacked. Manufacturers are responding and patching is becoming available for both APs and clients.

Action advised:

It is recommended that Wi-Fi network administrators responsible for wireless networks closely monitor the availability of software updates from vendors and patch as soon as possible. An intermediate measure is to disable 802.11r (aka Fast Roaming) on APs until an update is

available. Users should be made aware that until their phones, tablets and laptops are patched, there is a risk to the security of sensitive information transmitted over all WPA2 networks (including home, café, airport and other enterprise wireless networks). However WPA2 represents the best currently available technology and reversion to other techniques is not advised.

Source URL: <https://community.jisc.ac.uk/library/network-and-technology-service-docs/advisory-wpa2-key-reinstallation-attacks-vulnerability>

Links

[1] <https://www.eduroam.org/2017/10/18/key-reinstallation-attack-and-wpa2/>

[2] <https://www.krackattacks.com/>