An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

Wi-Fi Network Vulnerability

Information Notice

Reference: ComReg 17/88

Version: Final

Date: 25/10/2017

An Coimisiún um Rialáil Cumarsáide
Commission for Communications Regulation
1 Lárcheantar na nDugaí, Sráid na nGildeanna, BÁC 1, Éire, D01 E4X0.
One Dockland Central, Guild Street, Dublin 1, Ireland, D01 E4X0.
Teil | Tel +353 1 804 9600 Suíomh | Web www.comreg.ie

1. Recently, vulnerabilities have been identified in Wi-Fi Protected Access II ('WPA2'), a protocol that secures all modern Wi-Fi networks. The vulnerabilities are exploited using key reinstallation attacks (KRACKs) that can target any Wi-Fi client on laptops, smartphones, or smart home device. Hackers using KRACKs may be able to steal sensitive information (e.g. passwords, bank account details, credit card numbers).

2. The weaknesses are in the Wi-Fi standard itself and not in individual devices or their software. This means that any Wi-Fi enabled device using WPA2 is likely to be affected. Apple, Android, Linux and Windows based devices all use WPA2 and may be affected by some variant of the attacks.

3. The threat mainly relates to Wi-Fi clients but in limited circumstances the software on Wi-Fi routers may need to be updated. Irish network operators are assessing the risk to their Wi-Fi routers and will advise their customers if necessary action is required. An attack does not recover the password of your Wi-Fi network so changing the password of your Wi-Fi network does not prevent (or mitigate) the risk of an attack.

4. If you are concerned you should do the following:-

    i) Contact your network operator or visit their technical support website for more information.

    ii) For most home users, the priority should be updating clients such as laptops and smartphones. Users should wait for security updates on Wi-Fi devices to be announced (either by the device manufacturer or network operator) and install them as soon as possible. Some devices may no longer be supported by their manufacturer or may rarely receive updates. These devices may never receive an update.

    iii) Until updates are available, the risk can be minimised by treating all Wi-Fi access points, even at home, as an open unencrypted Wi-Fi network – similar to public Wi-Fi found in airports or cafés. When using public Wi-Fi, the use of a Virtual Private Network ('VPN') from a reputable provider is advised to ensure privacy and 'https' should be used for web applications where possible.

5. Further information on general online security questions/concerns is available on www.makeitsecure.ie.