OCTOBER 2017

blackfoot

BLACKFOOT NEWSFLASH

WPA2 KRACK vulnerability

Security researchers have publicised a serious vulnerability in WPA2, the encryption protocol relied on by most Wi-Fi networks.

On 16th October, security researchers announced a serious vulnerability in the WPA2 protocol. They have named the vulnerability KRACK (Key Reinstallation AttaCK).

The vulnerability was first discovered in 2016, and after further research was disclosed to vendors in July and August 2017.

Exploiting the vulnerability involves conducting a man in the middle (MiTM) attack in order to trick the victim's device into reinstalling an already used key. This is done by manipulating and replaying cryptographic 4-way handshake messages.

A successful exploitation of this vulnerability would potentially enable the attacker to inject ransomware or malware into web traffic, to manipulate data travelling over the wireless network, and to eavesdrop on sensitive information.

Fortunately, the attack cannot be conducted remotely, the attacker (or at least a device they are remotely controlling) needs to be within Wi-Fi range of your client device and your wireless access point.

A wide variety of systems are vulnerable, including: Android, iOS, macOS, Linux, OpenBSD, Windows, and IoT devices. Any network traffic that is encrypted such as HTTPS, VPN, SSH, TLS, or similar, is not exposed even in the case of a successful KRACK attack. However using HTTPS alone does not guarantee secure web browsing and transactions, because poorly configured or misconfigured SSL instances can be force-downgraded to HTTP using SSLstrip for example.

The attack does not generally expose the wireless network's pre-shared key.

What is the threat?

If your wireless access point or router uses WPA-TKIP or GCMP encryption, an attacker could potentially inject data into your unencrypted network traffic, such as malicious JavaScript code and malware downloads.

Devices running Android 6.0 or Linux with wpa_supplicant 2.4 (or earlier) are additionally vulnerable due weaknesses in their implementation of the WPA2 handshake mechanism.

Embedded and IoT devices are a particular concern. Many have wireless connectivity, and these devices are often not designed to be easily patched or updated. Also, in some businesses these devices are purchased outside of the IT's control, leading to a lowering of standards and a proliferation of devices and vendors.

How to tell if you are affected or vulnerable?

The weaknesses are in the Wi-Fi standard itself, and not in individual products or implementations. Therefore, all wireless networks are potentially vulnerable, including personal and enterprise networks, networks using the WPA or WPA2 protocols, and networks using AES encryption.

Unless patched with a known fix, assume that all WPA2 enabled Wi-Fi devices are vulnerable.

Microsoft has patched its Windows wireless code in its October batch of security updates, so Windows devices with those patches applied are protected. Apple have said that they will have security fixes for iOS and macOS available to the public within days, once beta testing is complete. Google have said that they are working on Android and ChromeOS patches.

Recommendations

Wireless access points and routers:

- Identify all your wireless access points/routers and their current OS/firmware version.
- Apply vendors' KRACK patches to your access points/routers as soon as they become available.
- Consider replacing those devices where patches are not forthcoming.

Wireless Clients (computers, tablets and smartphones:

- Identify all your wireless clients and their current OS/firmware version.
- Apply vendors' KRACK patches to your client devices as soon as they become available.
- Consider discontinuing the use of devices until they are patched.
- On unpatched phones and tablets, consider using 4G in preference Wi-Fi.
- Consider using wired Ethernet connections instead of Wi-Fi until computers and wireless access points are patched.
- Use mobile phone tethering in preference to untrusted wireless hot-spots.
- When accessing the internet from a business computer whilst away from the office, use a trusted VPN service.
- Only visit web sites which support HTTPS.
- Consider using a browser version or browser plug-in which enforces the use of HTTPS.

IoT and embedded wireless devices:

- Identify all your wireless embedded and IoT devices, and their current OS/firmware version.
- Apply vendors' KRACK patches to your embedded and IoT devices as soon as they become available.
- Consider discontinuing the use of devices until they are patched.
- Consider separating these devices onto a separate VLAN with no, or heavily restricted access to the rest of the network, where feasible.
- Where provided with an Ethernet port, consider using a wired Ethernet connection instead of Wi-Fi until patched.
- Consider certificate based authentication for those devices that support it.

People:

- Educate your colleagues (and family members) about the risks, and best practice recommendations.

Blackfoot's viewpoint

This is an industry-wide problem to do with how the Wi-Fi verifies users.

People are at limited risk due to most web connections now being secure. So most online purchases and banking are not at risk. However, corporates have an ever-growing reliance on Wi-Fi, whether for IOT, internal devices such as video conferencing and smart TV, or simply for ease of connection. It is likely you have some unencrypted data flowing across your internal Wi-Fi networks.

The good news is that hackers need to be physically located nearby, massively reducing the likelihood of attacks happening.

Further reading

https://www.krackattacks.com/
https://krebsonsecurity.com/2017/10/what-you-should-know-about-the-krack-wifi-security-weakness/#more-41189
https://techcrunch.com/2017/10/16/heres-what-you-can-do-to-protect-yourself-from-the-krack-wifi-vulnerability/

CVE identifiers

The following CVE identifiers will help you determine whether individual patches address KRACK vulnerabilities.
CVE-2017-13077: Reinstallation of the pairwise encryption key (PTK-TK) in the 4-way handshake.
CVE-2017-13078: Reinstallation of the group key (GTK) in the 4-way handshake.
CVE-2017-13079: Reinstallation of the integrity group key (IGTK) in the 4-way handshake.
CVE-2017-13080: Reinstallation of the group key (GTK) in the group key handshake.
CVE-2017-13081: Reinstallation of the integrity group key (IGTK) in the group key handshake.
CVE-2017-13082: Accepting a retransmitted Fast BSS Transition (FT) Reassociation Request and reinstalling the pairwise encryption key (PTK-TK) while processing it.
CVE-2017-13084: Reinstallation of the STK key in the PeerKey handshake.
CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake.
CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.
CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.

Contact your Blackfoot account manager to discuss early detection and assessment services, call 0845 805 2409 or email info@blackfootuk.com

Blackfoot UK Limited
Tel: 0845 805 2409
E-mail: info@blackfootuk.com
Web: www.blackfootuk.com

ADVISE >
ASSESS >
ASSURE >

This material is for information purposes only and does not take into consideration the particular circumstances or objectives of your business. Whilst every reasonable effort has been made to ensure the accuracy of the information in this document, Blackfoot UK Limited shall not be held liable for any errors or omissions.