Privasec RED
RED TEAMING & ADVANCED ETHICAL HACKING

KRACK – Wi-Fi Vulnerability

Fact Sheet v1.0 - 17th October 2017

BACKGROUND INFORMATION

- A significant flaw has been identified in a widely used protocol that protects modern Wi-Fi networks. It impacts the vast majority of Wi-Fi enabled devices, including routers, mobile phones, wearables, Internet of Things devices, communication devices, and almost everything else that has Wi-Fi, including your smart car.
- A malicious party must have access to a device within range of your Wi-Fi devices to exploit this vulnerability. Whilst it is currently complicated for an attacker to exploit this vulnerability, it expected to be automated and become a "click of a button" exploit (to be used by low-skilled attackers) within just a few days/weeks.
- This vulnerability works by effectively forcing devices to re-install encryption keys to the benefit of the attacker.

STEP ONE: DON'T PANIC

This isn't the first significant Wi-Fi vulnerability to be disclosed and it won't be the last.

Whilst this vulnerability has received ample media attention and is rather serious in nature, it currently requires a skilled and motivated attacker to be in the vicinity of your Wi-Fi network, and to be actively 'hacking' you. For most businesses the likelihood of such a scenario is low.

STEP TWO: ASSESS AND MINIMISE THE RISK TO YOU

Here are some actions you can consider taking to reduce the impact and likelihood of a successful attack on your network.

- Identify your Wi-Fi devices (including TVs, printers, etc.) and check if their vendors have already released patches. Prioritise patching access points and routers, but don't neglect your other Wi-Fi enabled devices.
- To prioritise your efforts, assess the location of your crown jewels and review your network segmentation controls to see if they can be accessed via Wi-Fi.
- For devices and networks transmitting highly sensitive data, and if you can afford to work on a wired network without business disruption, consider disabling your Wi-Fi until your devices are patched.

Business logic prevails: Consider the likelihood that you might be actively targeted by an attacker, the impact of such an attack, and act accordingly.

- If you are using an ISP branded modem-router (like a Telstra modem) that does not have a patch available, you can consider putting the router in bridged-mode, disabling the Wi-Fi, and connecting it to a separate Wi-Fi router that does have a patch available as an interim measure;
- If your business model allows it, prevent unpatched devices from connecting to your network until they can be patched;

A list of currently patched devices by manufacturer can be found here: https://www.bleepingcomputer.com/news/security/list-of-firmware-and-driver-updates-for-krack-wpa2-vulnerability/ - More lists will likely be released in the coming days.

STEP THREE: CHECK THAT YOUR HOUSE IN IS ORDER

We are seeing too much noise and panic-inducing media releases. Whilst such hype is probably not justified, it should serve as a reminder of a few good and simple practices that you should follow to keep your infrastructure healthy.

- Patch, Patch and Patch. Dust off your Vulnerability Management and Patching Framework and make sure it is relevant to today's landscape. Keep track of all your Wi-Fi devices and periodically check as patches become available to confirm that they are patched;
- Consider doing a Rogue Wireless Discovery exercise to locate any potential rogue and neighbouring Wi-Fi networks/devices in your premises, and to disable them where possible. If your PCI DSS compliance forces you to do one annually, now would be a good time to do it.
- Consider implementing certificate based authentication for services within your Wi-Fi network;
- Now is a good time to check for any legacy, unencrypted communications over your network, and to upgrade them to their more secure counterparts.
    - HTTP (use HTTPS only instead)
    - Telnet (use SSH or similar instead)
    - FTP (use SFTP or SCP instead)
    - Ensure all email traffic is encrypted by default as it is sent through the network
- You could enable MAC Address Whitelisting, but it if an attacker has the skills and motivation to exploit the KRACK vulnerability he or she can easily defeat MAC Whitelisting: unless you have a small Wi-Fi ecosystem, don't bother as the effort would outweigh the benefits.

DO YOU REQUIRE ADDITIONAL ASSURANCE?

Privasec can provide you with additional assurance and peace of mind.

If you would like us to review your patching practices, perform a Wireless Penetration Test, identify rogue and neighbouring wireless devices in your building, or review your current network architecture, please contact us for a personalised quote.