Gridware

KRACK WIFI VULNERABILITY

WHITE PAPER – OCTOBER 2017

Sydney Head Office
5 Martin Place
Sydney NSW 2000

Email
info@gridware.com.au

Telephone
d. +61 2 8405 7989

Introduction

A newly revealed Wi-Fi vulnerability that affects nearly all wireless device, from laptops to smart fridges, demonstrates the likelihood of a fundamental security flaw in the encryption protocol called WPA2, which may allow unauthorised viewing of Wi-Fi traffic. The flaw was published in July 2017 by a researcher who documented widespread vulnerabilities in various implementations of WPA2. All vendors of Wi-Fi equipment and clients where promptly notified through industry-level forums, for the purpose of developing patches. The public disclosure date was agreed for 16 October 2017.

Technical Overview

All Wi-Fi networks that leverage WPA2 are vulnerable. The vulnerability is due to implementation flaws rather than protocol-level weakness. Programmers did not anticipate and guard against a particular set of circumstances when writing the protocol.

Exploitation involves interception and replaying a portion of the initial four-way handshake of the protocol that is conducted when a client authenticates with an access point, and persuades a victim to reinstall a previously used key.

The following conditions limit the potential impact:

- The attacker needs to establish a man-in-the-middle (MITM) connection between the wireless access point and the victim;
- The vulnerability is a data link layer attack, which means the effective use of transport layer encryption will protect the data. Properly configured SSL/TLS connections and use of VPNs would in most cases prevent access to unencrypted data;
- Subsequent decryption attacks are required to view your data compromised by a KRACK vulnerability.

What you need to do

The Gridware intelligence team suggests that most attacks would focus on endpoints, meaning laptops, mobile phones and smart devices, rather than Wi-Fi access points such as routers. If your company runs Windows devices, it is imperative they install the latest patches released in October 2017 which should mitigate the KRACK vulnerability. Patches have also been released by Wi-Fi equipment manufacturers, including 'Netgear', 'Asus' and 'TP-Link' etc., IT teams should accelerate the issuing of those critical patches.

The risk still remains via third parties, (in addition to home networks, off-site offices, concierge desks, airport lounges etc.), so any connection to your company network should be conducted over VPN encryption between the device and the server.

Final Note

Work with your IT team and Information Security advisor to ensure:

1. All WPA2-connected systems in your company are patched to the latest firmware, including Windows October 10 patch and Internet of Things (IoT) devices, as soon as vendors release those security updates. Prioritise endpoint systems that access wireless networks, ie. employee devices.
2. Use transport layer encryption, such as HTTPS for websites, TLS for email, and internal VPNs, to protect sensitive data within networks using WPA2.
3. Finally, continue to use WPA2 in favour of other protocols. Our researchers conclude that despite these vulnerabilities, it remains the most secure option in comparison to other protocols such as WEP.

How Gridware Can Help You Today

Dedicated CISO Advisory

Providing dedicated governance and information security advisory resources to your business leaders with a clear evaluation of your requirements and structured deliverables to key projects covering:

- Cyber security evaluation & assessment
- Incident Response & Crisis Frameworks
- Cyber threat monitoring & reporting
- Vulnerability advisory, leak scout services
- Security initiatives (honeypots, sinkholds)
- Develop key policies and procedures
- Penetration testing
- Regulatory compliance

Cyber Security Strategy

We will work with your leadership team to devise a strategic framework for information security that aligns with your industry and peers and can support your business in areas covering:

- Cyber Security Frameworks (CFMs)
- Program direction in view of industry insight
- Assist with cyber operating models
- Project management
- Alignment with broader strategy
- Ongoing refinement of cyber security strategy and roadmap development

Cyber Risk Maturity Assessments

Undertake comprehensive risk assessments of existing controls, let us automate compliance reporting with industry standards, determine risk profile and tolerance, determine cyber maturity and develop road-maps for compliance with various industry standards (ISO27001, NIST, SOC2).