Security Advisory Report - OBSO-1711-01

WPA2 Protocol Four-way Handshake Handling MitM Issue (KRACK attack)

Creation Date: 2017-10-23 10:03:46
Last Update: 2018-02-21 13:03:40

Summary

Mathy Vanhoef of the imec-DistriNet research group of KU Leuven discovered multiple vulnerabilities in the WPA protocol, used for authentication in wireless networks.
Those vulnerabilities applies to both the access point (implemented in hostapd) and the station (implemented in wpa_supplicant).

An attacker exploiting the vulnerabilities could force the vulnerable system to reuse cryptographic session keys, enabling a range of cryptographic attacks against the ciphers used in WPA1 and WPA2.

http://seclists.org/bugtraq/2017/Oct/25

Details

Wi-Fi Protected Access (WPA, more commonly WPA2) handshake traffic can be manipulated to induce nonce and session key reuse, resulting in key reinstallation by a wireless access point (AP) or client. An attacker within range of an affected AP and client may leverage these vulnerabilities to conduct attacks that are dependent on the data confidentiality protocols being used.
Attacks may include arbitrary packet decryption and injection, TCP connection hijacking, HTTP content injection, or the replay of unicast and group-addressed frames. These vulnerabilities are referred to as Key Reinstallation Attacks or "KRACK" attacks.

http://www.kb.cert.org/vuls/id/228519

The attack is against the 4-way handshake of the WPA2 protocol. This handshake is executed when a client wants to join a protected Wi-Fi network, and is used to confirm that both the client and access point possess the correct credentials (e.g. the pre-shared password of the network).
At the same time, the 4-way handshake also negotiates a fresh encryption key that will be used to encrypt all subsequent traffic. Currently, all modern protected Wi-Fi networks use the 4-way handshake. This implies all these networks are affected by (some variant of) our attack. For instance, the attack works against personal and enterprise Wi-Fi networks, against the older WPA and the latest WPA2 standard, and even against networks that only use AES.

https://www.krackattacks.com/

Android and Linux can be tricked into (re) installing an all-zero encryption key.

http://seclists.org/bugtraq/2017/Oct/25

https://www.krackattacks.com/

Attack type

CWE-323: Reusing a Nonce, Key Pair in Encryption

The following CVE IDs have been assigned to document these vulnerabilities in the WPA2 protocol:

CVE-2017-13077: reinstallation of the pairwise key in the Four-way handshake

CVE-2017-13078: reinstallation of the group key in the Four-way handshake

CVE-2017-13079: reinstallation of the integrity group key in the Four-way handshake

CVE-2017-13080: reinstallation of the group key in the Group Key handshake

CVE-2017-13081: reinstallation of the integrity group key in the Group Key handshake

CVE-2017-13082: accepting a retransmitted Fast BSS Transition Reassociation Request and reinstalling the pairwise key 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

Impact

An attacker within the wireless communications range of an affected AP and client may leverage these vulnerabilities to conduct attacks that are dependent on the data confidentiality protocol being used.

Impacts may include arbitrary packet decryption and injection, TCP connection hijacking, HTTP content injection, or the replay of unicast, broadcast, and multicast frames.

http://www.kb.cert.org/vuls/id/228519

PoC:

https://www.krackattacks.com/

Detailed paper:

https://www.krackattacks.com/

Affected Products

The only Unify product that uses WLAN is the WL3 phone.

A correction is available since 2018-02-13:

OpenStage WL3	V1 R1.4.0 (6.0.7)
OpenStage WL3 Plus	V1 R1.4.0 (6.0.7)
OpenStage WL3 Wireless Service Gateway	V1 R1.4.0 (4.4.2)

Recommended Actions

This attack is only possible if an attacker can use a Man-in-the-Middle attack.
Usage of VPNs or HTTPS prevents these attacks.

This attack requires considerable effort, so priority is medium.

All systems should be patched.

WL3 phones should be used with TLS and SRTP avoiding Man-in-the-Middle attack

The update for WL3 phone should be installed as soon as possible.

References

https://www.krackattacks.com/

https://papers.mathyvanhoef.com/ccs2017.pdf

http://seclists.org/bugtraq/2017/Oct/25

http://www.kb.cert.org/vuls/id/228519

https://www.security-insider.de/potentieller-angriff-auf-wpa2-entdeckt-a-653276/?cmp=nl-36&uuid=B5F51171-63BC-46AD-B9F14E20B4337135

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-13077

https://www.blackhat.com/docs/webcast/08242017-securely-implementing-network2.pdf

https://www.engadget.com/2017/10/16/wifi-vulnerability-krack-attack/

https://www.theguardian.com/technology/2017/oct/16/wpa2-wifi-security-vulnerable-hacking-us-government-warns

https://www.theregister.co.uk/2017/10/16/wpa2_krack_attack_security_wifi_wireless/

https://www.heise.de/security/artikel/KRACK-so-funktioniert-der-Angriff-auf-WPA2-3865019.html

Revision history

- 2017-11-03 [Reiff Ulrich]:

  Release

- 2017-10-27 [Reiff Ulrich]:

  Update Draft

- 2017-10-23 [Reiff Ulrich]:

  First Draft

Contact and Disclaimer

OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com