Security Alert - Krack attacks exposure of WPA2 Technicolor devices

TLP: GREEN

(see https://www.us-cert.gov/tlp)

Summary

By making use of a model-based approach, researchers from K.U Leuven University have identified several flaws in the Wi-Fi protocol. These vulnerabilities constitute a new class of attack on the 4-way handshake used in all flavors of WPA2.

This industry-wide issue affects all products implementing Wi-Fi in a theoretical way, and some of the clients (Wi-Fi supplicant) in a practical way.

Exposure

A set of vulnerabilities allowing for an attack dubbed key reinstallation attack (KRACK) has been identified in the Wi-Fi Protected Access 2 (WPA2) protocol. An attacker within range of the victim could exploit it in order to force the reinstallation of a key that is already in use, and thus reset nonces and/or replay counters associated to this key. Several 4-way handshakes, used for different features of the protocol, have been identified with such flaws.

Impact

The precondition is to be in vicinity of the victim. The impact differs whether the Wi-Fi device acts as an Access Point or a Supplicant. The worst case scenario implies the ability to force the key used by a Supplicant to the zero value. Even in this case, the primary key (WPA2 password) is not compromised.

Common Vulnerability Scoring System

This impact is assessed in the worst case scenario (supplicant installing an all-zero key), with immediate impact on the confidentiality of the LAN. Yet, in the context of the Technicolor devices, the supplicants are Set-top-box and OTT devices, where the video content remains protected at applicative level. Hence, no Technicolor device have been found affected at this level of risk.

CVSS Base Score	5.8
CVSS Temporal Score	5.2
CVSS Environmental Score	6.2
Overall CVSS Score	6.2

CVSS v2 Vector

(AV:A/AC:H/Au:N/C:C/I:P/A:P/E:POC/RL:U/RC:C/CDP:LM/TD:H/CR

Security Office

security@technicolor.com

Security Alert

Affected Products

Reference	CVSS Overall score	CVE
OWA130 TG233 TG234	4.6	CVE-2017-13077 CVE-2017-13078 CVE-2017-13079 CVE-2017-13080 CVE-2017-13081 CVE-2017-13084 CVE-2017-13086 CVE-2017-13087 CVE-2017-13088
UIW4010ECH DWT765TI UZW4010TIM DWT765GEN DCI765EKT DWT765LMT DWT765EKT DWI765YES	4.6	CVE-2017-13077 CVE-2017-13078 CVE-2017-13079 CVE-2017-13080 CVE-2017-13081 CVE-2017-13086 CVE-2017-13087 CVE-2017-13088
	1.4	CVE-2017-13082

History Version

Version	Date	Change Log

:L/IR:M/AR:H)

CVSS for the more theoretical attacks

CVE	Target	Description	CVSS Base Score	Overall CVSS Score	CVSS v2 Vector
CVE-2017-13077 CVE-2017-13078 CVE-2017-13079 CVE-2017-13080 CVE-2017-13081 CVE-2017-13084 (not applicable to Android) CVE-2017-13086 CVE-2017-13087 CVE-2017-13088	Supplicant	A key re-installation attack is possible on several 802.11i 4-way handshake messages of the WPA and WPA2 protocols, allowing an unauthenticated, adjacent attacker to force a supplicant to reinstall a previously used pairwise key. Or, an all-zero key can be forced, but the content remains protected at applicative level by Content Access System, or Digital Right Management systems.	4.3	4.6	(AV:A/AC:H/Au:N/C:P/I:P/A:P/E:POC/RL:U/RC:C/CDP:L/TD:H/CR:L/IR:M/AR:H)

3.0	18 Oct 2017	Providing more accurate analysis of overall CVSS score, depending on target nature. Updating list of products. Adding link to CERT-CC page. Adding Wi-Fi doctor as not affected.
2.0	17 Oct 2017	Clarifying section related to Fast BSS Transition Handshake attack. Adding mention of Technicolor/Thomson routers as generally not affected.
1.0	17 Oct 2017	First public version.

TLP
GREEN

CVE-2017-13082	Access Point	Wi-Fi Protected Access (WPA and WPA2) that supports IEEE 802.11r, and allows reinstallation of the Pairwise Transient Key (PTK) Temporal Key (TK) during the fast BSS transmission (FT) handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.	4.3	1.4	(AV:A/AC:H/Au:N/C:P/I:P/A:P/E:POC/RL:W/RC:C/CDP:LM/TD:L/CR:L/IR:M/AR:H)

Comment

As a member, Technicolor follows Wi-Fi alliance security guidance in testing these vulnerabilities on its products and will update this document upon further analysis.
Even with this attack, WPA2 remains far more secure than any use of Wi-Fi open spot. Security at applicative level, using for instance HTTPS, also ensures the protection of the applications data regardless of these vulnerabilities.
Only Wi-Fi supplicants are vulnerable. Personal routers configured as Wi-Fi Access Point are not affected, except when supporting Fast BSS Transition handshake (802.11r). Fast BSS Transition handshake (802.11r) is usually not supported on personal routers, because this feature is intended to minimize roaming time between several APs in a managed network. This limits the number of Technicolor devices potentially affected.
Technicolor will continue to analyze these weaknesses, and will propose patches in priority on devices affected with highest CVSS overall score.
The list of Technicolor devices confirmed affected is provided here below:

- TG233, TG234 in STA mode (station)
- OWA0130 in STA and AP/STA mode (station, repeater)
- Android 6.0.1 OTT devices:
    - UIW4010ECH
    - DWT765TI
    - UZW4010TIM
    - DWT765GEN
    - DCI765EKT
    - DWT765LMT
    - DWT765EKT
    - DWI765YES

All Thomson/Technicolor gateways not supporting 802.11r are not vulnerable.

Wi-Fi doctor is not affected.

Workaround

Since these weaknesses rely in the protocol itself, there is no workaround, except for CVE-2017-13082, where the workaround is to disable fast roaming.

Exploitation

Technicolor Security Office is not aware of any malicious use of the vulnerability that is described in this note.

Related links

- https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-security-update
- https://www.blackhat.com/docs/webcast/08242017-securely-implementing-network2.pdf
- https://www.krackattacks.com
- https://www.kb.cert.org/vuls/id/228519

Legal advisory

This document is provided on an "as is" basis. It does NOT imply any kind of guarantee or warranty. Technicolor reserves the right to update this document at any time, to reflect new information.

Any question on this advisory can be sent to the Technicolor Security Office.