ALE Security Advisory No. SA-C0060 Ed. 01

WLAN Handsets - WPA2 Key Reinstallation Vulnerabilities - KRACK Attack

Summary

Common industry-wide flaws in WPA2 key management may allow an attacker to decrypt, replay, and forge some frames on a WPA2 encrypted network. The accompanying FAQ document provides more extensive details.

Description of Issue

A vulnerability affecting the WPA2 802.11 protocol has just been announced on the Internet. Known as KRACK, it is a group of ten vulnerabilities that all concern the encryption negotiation phase in the WPA2 protocol, and extensively WPA protocol.
This vulnerability allows an attacker within the Wifi range of a given victim, to break the encryption implemented by WPA2, and then listen or inject traffic into this victim's Wifi connection.
This vulnerability is a concern when the user does not use a VPN, or in case of not using SSL/HTTPS based application protocols, to protect network traffic within a Wifi connection.
This can be the case, for example, in enterprise context where internal Wi-Fi access is offered to employees. In this case, a visitor could use this vulnerability to eavesdrop on private employees traffic and steal sensitive data (password, etc.).

For more information:

- Official website describing the vulnerability: https://www.krackattacks.com
- Description VU#228519 by CERT-CC: https://www.kb.cert.org/vuls/id/228519

List of CVEs for vulnerability KRACK:

- **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.

Status on Alcatel-Lucent Enterprise WLAN Handset Products

List of products and releases **concerned** (or affected):

Product Name	Release
8118 WLAN Handset	up to version 5.6.1
8128 WLAN Handset	up to version 5.6.1
8128 SE WLAN Handset	up to version 5.6.1

Risks limitation

Discoverer claims that "We are not in a position to determine if this vulnerability has been (or is being) actively exploited in the wild," Vanhoef says. CERT's advisory didn't include any information about whether KRACK is being exploited in the wild, either. There are no automated tools that allow someone to deliver this attack in a simple way today. Now for some somewhat settling news: Iron Group CTO Alex Hudson says an attacker needs to be on the same Wi-Fi network as you in order to carry out any nefarious plans with KRACK. "You're not suddenly vulnerable to everyone on the internet," he says.

Nevertheless, make sure to apply appropriate software patches or available workarounds on your infrastructure equipment, or access points to limit the risks of exploiting infrastructure side vulnerability until the software corrections are available for your handset client products.

Resolution for Alcatel-Lucent Enterprise Affected Products

ALE is working on the related software corrections and will publish updates as soon as possible on our ALE public website for security advisories: https://www.al-enterprise.com/en/support/security-advisories

Please keep checking the page for the latest information.

History

Ed.01 (2017 October 18th): creation