MITIGATIONS FOR KEY REINSTALLATION ATTACKS AGAINST WI-FI PROTECTED ACCESS II (WPA2)

DISCUSSION

On October 16, 2017, a vulnerability in the Wi-Fi Protected Access II (WPA2) mechanism used for authentication and session key agreement was released. [1,2] The vulnerability affects the following WPA2 handshakes: the Four-way, Group Key, Fast BSS Transition (FT), Peerkey, Tunneled Direct-Link Setup (TDLS), and Wireless Mesh Network (WMN) Sleep Mode Response handshakes.

The attacker must be within wireless communications range of the device being attacked in order to manipulate and replay handshake messages to force the attacked device to reinstall the previously installed key. The key reinstallation resets the nonce and replay counters, which violates an important security tenet of stream ciphers: a nonce must be a non-repeating value. The key and nonce reuse does not result in recovery of the actual session key, but results in the reuse of the same derived keystream.

All Wi-Fi capable devices are affected, however, the severity of the impact changes depending on the handshake type, confidentiality protocol, and the operating system. For example, for the Four-way or Fast BSS handshake using Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP), the attacker would be able to replay and decrypt some traffic. For those same handshakes using TKIP or Advanced Encryption Standard – Galois/Counter Mode Protocol (AES-GCMP), the attacker would be able to replay, decrypt traffic, and inject arbitrary packets. For wpa_supplicant versions 2.4, 2.5 and 2.6, rather than reinstalling the previously installed key, the attack sets the key to all zeros.

MITIGATION ACTIONS

- Install patches to both the clients and Access Systems as soon as they are made available. [3,4,5]
  Relevant CVEs [2]: CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13084, CVE-2017-13086, CVE-2017-13087, and CVE-2017-13088.
- Disable Fast BSS Transition on Access Systems until patches are available to prevent the FT handshake attack.
- Temporarily use only AES-CCMP until patches are available.
- Install an underlying virtual private network until patches are available.
- Do not use modes requiring generation of a Peerkey.

REFERENCES

[1] Mathy Vanjoef and Frank Piessens. 2017. Key Reinstallation Attacks: Breaking WPA2 by forcing nonce reuse. www.krackattacks.com.

[2] CERT/CC. 2017. Vulnerability Note VU#228519:Wi-Fi Protected Access (WPA) Handshake Traffic Can Be Manipulated to Induce Nonce and Session Key Reuse. www.kb.cert.org/vuls/id/228519.

[3] Aruba Networks[1]. 2017. Aruba Product Security Advisory. Advisory ID: Aruba-PSA-2017-007. www.arubanetworks.com/assetts/alert/aruba-psa-201-007.txt.

[4] Cisco[2]. 2017. Multiple Vulnerabilities in Wi-Fi Protected Access and Wi-Fi Protected Access II. tools.cisco.com/security/center/content/ciscosecurityadvisory/cisco-sa-20171016-wpa

[1] Aruba Networks is a registered trademark of Hewlett Packard Enterprise Development LP

[2] Cisco is a registered trademark of Cisco Systems, Inc.

[5] Intel[3]. 2017. One or more Intel Products affected by the W-Fi Protected Access II (WPA2) protocol vulnerability. security-center.intel.com/advisory.aspx?intelid=intel-sa-00101&languageid=en-fr

DISCLAIMER OF WARRANTIES AND ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

CONTACT INFORMATION

Client Requirements and General Cybersecurity Inquiries:

Cybersecurity Requirements Center

410-854-4200

Email: Cybersecurity_Requests@nsa.gov

[3] Intel is a registered trademark of Intel Corporation