HMSSAR-2017-10-17-001

Publication date: 18 October, 2017
Last update: 27 August, 2018

WLAN Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2

Overview

On October 16th, 2017, a research paper with the title of "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2" was made publicly available. This paper discusses seven vulnerabilities affecting session key negotiation in both the Wi-Fi Protected Access (WPA) and the Wi-Fi Protected Access II (WPA2) protocols. These vulnerabilities may allow the reinstallation of a pairwise transient key, a group key, or an integrity key on either a wireless client or a wireless access point. Additional research also led to the discovery of three additional vulnerabilities (not discussed in the original paper) affecting wireless supplicant supporting either the 802.11z (Extensions to Direct-Link Setup) standard or the 802.11v (Wireless Network Management) standard. The three additional vulnerabilities could also allow the reinstallation of a pairwise key, group key, or integrity group key.

Impact

Successful exploitation of this vulnerability may allow a remote attacker to cause a denial of service or execute code on the target device.

Affected products and versions

Anybus Wireless Bolt and Anybus Wireless Bridge II

An update has been released with firmware v1.5.3 which provides a fix for the KRACK vulnerability. The product is now no longer vulnerable to the KRACK attacks.

Anybus Wireless Bridge (legacy), Ethernet Port Adapter (legacy) for WLAN

The test suite released by Wi-Fi alliance has been used in a test setup and the product is vulnerable to the group key reinstallation attack (Wi-Fi alliance tests CVE-2017-13080 and CVE-2017-13078) only, but not to the other attacks. Regarding the group key attack, it is demonstrated with only one station associated to an AP and can maybe be orchestrated with 2-3 stations after which it gets too complex. Typical (enterprise) installations have more stations connected to each AP.

Severity / CVSS Score

TBD

HMS Recommendations

Update Anybus Wireless Bolt and Bridge to the latest firmware, at least v1.5.3.

Product updates

Anybus Wireless Bolt and Anybus Wireless Bridge II:
The latest firmware can be downloaded here: https://www.anybus.com/support/file-doc-downloads/select-wireless-type

Anybus Wireless Bridge (legacy), Ethernet Port Adapter (legacy) for WLAN:
The are no product updates available.

Additional information

The security issue was discovered by Mathy Vanhoef of imec-DistriNet, KU Leuven and was first reported here: https://www.krackattacks.com/