WPA2 Key Reinstallation Attack (KRACK) vulnerabilities in Hirschmann BAT devices

Date: June 6, 2018
Version: 1.1
References: 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, CVE-2017-13088

Executive Summary

An attacker can force WPA1/WPA2-enabled wireless LAN devices into reinstalling the encryption key. This leads to nonce reuse and compromises the security of the underlying stream ciphers.

Details

Reference	Vulnerability Description	CVSSv3 Score
CVE-2017-13077	Reinstallation of the pairwise encryption key (PTK-TK) in the 4-way handshake.	6.8
CVE-2017-13078	Reinstallation of the group key (GTK) in the 4-way handshake.	5.3
CVE-2017-13079	Reinstallation of the integrity group key (IGTK) in the 4-way handshake.	5.3
CVE-2017-13080	Reinstallation of the group key (GTK) in the group key handshake.	5.3
CVE-2017-13081	Reinstallation of the integrity group key (IGTK) in the group key handshake.	5.3
CVE-2017-13082	Accepting a retransmitted Fast BSS Transition (FT) Reassociation Request and reinstalling the pairwise encryption key (PTK-TK) while processing it.	8.1
CVE-2017-13084	Reinstallation of the STK key in the PeerKey handshake.	6.8
CVE-2017-13086	Reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake.	6.8
CVE-2017-13087	Reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.	5.3
CVE-2017-13088	Reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.	5.3

CVSSv3 score source: National Vulnerability Database (NVD), November 07, 2017.

Impact

CVE-2017-13082 describes a vulnerability in infrastructure devices that support 802.11r “Fast BSS Transition”, the other CVEs describe various vulnerabilities in client devices. Since it can affect both infrastructure devices and clients, customers need to update all affected WLAN devices, it is not sufficient to only update either the access points or the clients.

The concept behind all these vulnerabilities is a reinstallation of an encryption key and consequently a reuse of nonces in the stream cipher. A successful exploit can lead to replay, decryption or forgery of packets. The packet direction that is vulnerable depends on whether an infrastructure or a client device is attacked.

A successful exploit does not compromise the authentication mechanisms of WPA2. In particular, an attacker cannot recover information about credentials such as certificates or Pre-shared Keys (PSK).

Affected Products

Brand	Product Line / Platform	Product	Version	Affected by
Hirschmann	Wireless	OpenBAT-R/F, BAT450-F	HiLCOS 9.12.5700-RU2 and lower	CVE-2017-13082
Hirschmann	Wireless	BAT867-R	HiLCOS 9.14.5700-RU2 and lower	CVE-2017-13077 CVE-2017-13080 CVE-2017-13082
Hirschmann	Wireless	BAT-C	BAT-C SW 2.5.1	CVE-2017-13078 CVE-2017-13080

Other Hirschmann products are not affected by the vulnerabilities listed in this document.

Solution

Update to one of the software versions below:

Brand	Product Line / Platform	Product	Version
Hirschmann	Wireless	OpenBAT-R/F, BAT450-F	HiLCOS 9.12.5750-RU3
Hirschmann	Wireless	BAT867-R	HiLCOS 9.14.5750-RU3
Hirschmann	Wireless	BAT-C	No fix planned

The updated software is available from
https://hirschmann-support.belden.com/
and
https://www.e-catalog.beldensolutions.com/link/57078-24455-278205-377857-400465/en/conf/0.

For Help or Feedback

To view all Belden Security Advisories and Bulletins or to report suspected security vulnerabilities, go to https://www.belden.com/security.
For technical support and other requests, please visit https://hirschmann-support.belden.com/

Related Links

- [1] https://www.krackattacks.com/

Disclaimer

THE SECURITY BULLETIN, AND INFORMATION CONTAINED HEREIN, ARE PROVIDED ON AN "AS IS" BASIS AND DO NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE BULLETIN, AND INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED FROM THE BULLETIN, IS AT YOUR OWN RISK. INFORMATION IN THIS BULLETIN AND ANY RELATED COMMUNICATIONS IS BASED ON OUR KNOWLEDGE AT THE TIME OF PUBLICATION AND IS SUBJECT TO CHANGE WITHOUT NOTICE. BELDEN RESERVES THE RIGHT TO CHANGE OR UPDATE BULLETINS AT ANY TIME.

Revisions

V1.0: October 24, 2017	Advisory created
V1.1: June 6, 2018	Bulletin created