Are Hirschmann WLAN products affected by the vulnerabilities described in CVE-2017-13077, -13078, -13079, -13080, -13081, -13082, -13084, -13086, -13087, -13088, used for the so called KRACK attack?

- 2018-02-09 - BAT

Hirschmann WLAN devices are affected by the vulnerability described in CVE-2017-13082 if they use WPA as security method and simultaneously have “Fast Roaming” enabled. Additionally, the BAT867R is affected by CVE-2017-13077 when used in client mode.

This allows an attacker in range of both the access point and a client of a WLAN installation to trick either the access point (CVE-2017-13082) or the client (CVE-2017-13077) into reinstalling the Pairwise Temporal Key, which partly compromises the encryption of WPA. (Note that the authentication, independent of whether it uses a pre-shared key (PSK) or EAP, is not affected by KRACK: an attacker cannot recover the pre-shared key of a WLAN installation.)

Hirschmann is working on updated software for its WLAN products and is going to announce details in the following days. Until the fix can be rolled out, we recommend customers turn off “Fast Roaming” and do not use devices in client mode to mitigate the effects of CVE-2017-13082 and CVE-2017-13077. If customers must use “Fast Roaming” or client mode, they can still use end-to-end encrypted communication like HTTPS, other TLS-based protocols, or VPNs, such as IPsec or OpenVPN, without risk.