KRACK Vulnerability

The WPA2 weakness using key reinstallation attacks (KRACK) discovered by Mathy Vanhoef of imec-DistriNet works against all modern protected Wi-Fi networks by allowing attackers to read information that was previously assumed to be safely encrypted.

The main attack is against the 4-way handshake of the WPA2 protocol which is executed when a client wants to join a protected Wi-Fi network, and is used to confirm that both the client and access point possess the correct credentials.

Instead of using this vulnerability for malicious action, Mathy Vanhoef properly documents and releases the following Common Vulnerabilities and Exposures (CVE) identifiers to track which products are affected by specific instantiations of 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) Re-association Request and reinstalling the pairwise encryption key (PTK-TK) while processing it.
- CVE-2017-13084: Reinstallation of the STK key in the Peer Key handshake.
- CVE-2017-13086: Reinstallation of the Tunnelled Direct-Link Setup (TDLS) Peer Key (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.

Most of these attacks target client devices, and standard Access Points are not affected, except when establishing a Wireless Distribution System (WDS) link between two APs turning the remote end in station (AP STA) mode.

The primary impact is to Android versions v6.0 or later and Linux client devices, while IOS and Windows are reported to be safe. Microsoft, Apple, Google, Intel, and other major vendors have been working on fixing these vulnerabilities for a few months now.

In addition to the vulnerabilities in WDS, CVE-2017-13082 targets Fast BSS Transition (FT) implemented in the 802.11r fast roaming protocol and affects both clients and Access Points.

Proxim Wireless Corporation. 2114 Ringwood Ave, San Jose, CA 95131, USA. P 408.383.7700

Proxim Wireless and KRACK

ORiNOCO® 802.11n and 802.11ac Access Point (AP-9100, AP-9100R, QB-9100, AP-8100) and Tsunami Cross Point (XP-101x0) support WDS communications based on AP STA mode. If a WDS link is established between APs, then the KRACK vulnerability may be exploited. For all these Access Points, Proxim Wireless released patch firmware correcting the WDS vulnerability. This patch firmware is available for download on the Proxim Wireless support site: http://support.proxim.com

ORiNOCO® AP-9100 and AP-9100R implement the 802.11r fast roaming protocol. The Fast Roaming vulnerability is also corrected by the above mentioned patch firmware.

ORiNOCO® USB-9100 adapter is only supported for Windows based computers and takes advantage of Windows tools including WPA2 security module. Thus, as Microsoft Windows is not affected by KRACK, it is safe to keep using ORiNOCO® USB-9100.

Legacy ORiNOCO® AP-700 and AP-4000 WDS and Mesh implementation is not based on AP STA mode and thus it is not subject to the KRACK vulnerability.

All Tsunami® products, which are based on Proxim's proprietary WORP® protocol, are not affected by the KRACK vulnerability as it doesn't use the 4-way handshake used in the WI-FI protocol.

Moreover, WORP also implements an additional authentication mechanism between devices. Thus all Tsunami devices are not subject to KRACK vulnerability.

Proxim will not be supplying security patches for affected End of Life / End of Support ORiNOCO® products not mentioned in this document.

Please see http://support.proxim.com/s/article/KRACK-Wi-Fi-Vulnerability-Information-Center for details and ways to mitigate these issues.

Proxim Wireless Corporation. 2114 Ringwood Ave, San Jose, CA 95131, USA. P 408.383.7700

About Proxim Wireless

Proxim Wireless Corporation (OTC Markets: PRXM) provides Wi-Fi®, Point-to-Point and Point-to-Multipoint wireless network technologies for wireless Internet, video surveillance and backhaul applications. Our ORiNOCO® and Tsunami® product lines are sold to service providers, governments and enterprises with over 2.5 million devices shipped to 250,000+ customers in more than 90 countries worldwide. Proxim is ISO 9001:2015 certified. For more information, visit www.proxim.com. For investor relations information, e-mail ir@proxim.com or call +1(408) 383 7615.

To find out more about Proxim Wireless, please visit www.proxim.com or follow us on Twitter, LinkedIn and Google+. Like us on Facebook or go to our YouTube page for latest videos.

Safe Harbor Statement

Statements in this press release that are not statements of historical facts are forward-looking statements that involve risks, uncertainties, and assumptions. Our actual results may differ materially from the results anticipated in these forward-looking statements. The forward-looking statements involve risks and uncertainties that could contribute to such differences, including difficulties in overcoming the network installation and operational challenges relating to any specific customer or geographical area; factors beyond our control such as weather, geographic, governmental, and interference issues that may increase the costs and difficulties of wireless deployments; specific requirements of a given customer in their specific situations; whether the deployment will achieve the desired objectives of any given customer; changes in the timing, features, and other characteristics of products Proxim expects to introduce; and difficulties or delays in supplying products with the features, performance, compliances, certifications, cost, price, quality, and other characteristics desired by customers. Further information on these and other factors that could affect Proxim's actual results is contained in the filings made by Proxim with the OTC Markets (available at www.otcmarkets.com), including without limitation in the Annual Report filed by Proxim on March 30, 2010, and is and will be contained in its other public statements, which may be available on Proxim's website (www.proxim.com).

Proxim Wireless Corporation. 2114 Ringwood Ave, San Jose, CA 95131, USA. P 408.383.7700