Security Advisory
KRACK WPA/WPA2 Vulnerability

Introduction:
On October 16, 2017, a research paper was made public by Dr. Mathy Vanhoef of IMEC-DistriNet Research Group of KU Leuven that uncovered a security vulnerability in key negotiations in both the Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) protocols. The vulnerability, most commonly known as KRACK, is associated with the process used for negotiating encryption keys used by the client and access point.

Scope of Impact:
Access points and Wi-Fi clients are impacted by this vulnerability. It affects client to access point communication only, not access point to client. If exploited, it enables eavesdropping on communications from the client to AP direction for someone in range of a Wi-Fi network. Of the most common operating systems, Android devices have exposure to the issue. Microsoft Windows and iOS are only affected if 802.11r roaming is in use. In the end, WPA/WPA2 are not fundamentally broken by the issue and the vulnerability can be addressed with a software patch.

Current Status:
Riverbed Xirrus was made aware of the vulnerability in advance of the public notice and has conducted an evaluation of the impact to Xirrus product portfolio. We are working to take necessary actions to address the vulnerability as soon as possible in access point software patches.

Action to take:
In advance of a patch, we recommend the following for Riverbed Xirrus customers:

- Turn off TKIP encryption – this is the most important precaution to take. While TKIP usage is not common, check if it is enabled on your network.
- Ensure your Wi-Fi clients are patched and kept up to date. Some client manufacturers have already issued patches while others will be rolling out soon.
- Turn off 802.11r feature if you are using it (disabled by default in Xirrus software)
- Turn on 802.11w protected management frames

In general, we recommend using https and/or VPNs as a best practice when connecting to public or other Wi-Fi networks outside your company/organization.

Stay tuned for more information from Riverbed Xirrus regarding this vulnerability.

For more information:
As soon as the patch is released, it will be made available through the Xirrus Support Community.

The Xirrus Customer Support Community contains a wealth of information regarding Xirrus products including the latest software releases, security bulletins, how-to guides, product announcements, tech tips and 24/7 access to your support tickets. You may log in and ask additional questions at support.xirrus.com.

Resources:

- Customer Support Community

If you have any questions regarding this security vulnerability please contact Customer Support via the Support Community.

Thank you,

Xirrus Customer Support
support@xirrus.com

United States and Canada	+1.800.947.7871 (US Toll Free) or +1.805.262.1600 (Direct)
Europe, Middle East, and Africa	+44.20.3239.8644
Australia	1.300.947.787 (Within Australia)
Asia and Oceania	+61.2.8006.0622
Latin, Central, and South America	+1.805.262.1600