# Security Advisory
# KRACK WPA/WPA2 Vulnerability

Updated 10/25/17

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

**Scope of Impact:**

While both Wi-Fi access points and Wi-Fi clients using WPA or WPA2 security are impacted, most of the vulnerabilities affect client devices. If exploited, it enables potential eavesdropping on communications from the client-to-AP (but not access point-to-client) 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 devices are only affected if 802.11r roaming is in use. WPA/WPA2 security is 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. In the meantime, workarounds are available by disabling specific features on the access point.

**Action to Take:**

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

- Turn off 802.11r roaming if possible. 802.11r is disabled by default in Xirrus software. Disabling 11r removes the AP vulnerability for Windows and iOS devices. Windows and iOS clients also still need to be updated to remove all vulnerabilities.
- Turn off WDS if possible. Together with disabling 802.11r, this will eliminate the vulnerability for Xirrus access points as a workaround until a patch is issued.
- Turn off TKIP encryption. 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 issued patches while others will be rolling out soon.

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.

**Security Fix:**
We anticipate the release of a security patch for mainline Xirrus AOS software by October 30, 2017. Other software branches will receive security patches soon after. We are acting with utmost priority to ensure the security of Xirrus networks.

For Xirrus customers using XMS-Enterprise, the patch will be made available through the Xirrus Customer Support Community as soon as it is available. From there it can be downloaded and your access points upgraded.

For Xirrus customers using XMS-Cloud, there are two options:
- By default, Xirrus will automatically push the access point software update within 2 days of the release of the patch during a normal maintenance window.
- If you want to control when your access points are updated, set the maintenance window under the upper right hand drop down in Settings – Firmware Upgrades.

If you have any questions or concerns about the upgrade process, contact Customer Support via the Support Community.

**Customer 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. 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 |