KRACK WPA/WPA2 Security Vulnerability
Frequently Asked Questions (FAQ)
October 16, 2017

1. **Does this vulnerability only impact networks using the TKIP cipher?**
   No, all cipher suites such as TKIP, AES and GCMP are impacted by this vulnerability.

2. **Do we need another protocol, such as a new version of WPA2?**
   No, the existing protocol is secure with appropriate implementation modifications. Both client and access point software can be patched with software fixes to address the issue.

3. **Does this vulnerability impact both WPA and WPA2?**
   Yes, both are impacted by this vulnerability which exists in the key handshake.

4. **Are my Wi-Fi devices – smartphones, laptops, tablets, etc. – vulnerable?**
   Likely your devices are vulnerable until you have implemented appropriate security updates from the device vendors. Contact your vendors to validate.

5. **Should I shut down my Wi-Fi network until this is fixed?**
   No, the vulnerability is in the 4-way handshake that is part of the process for a device to connect to a Wi-Fi network. It does not exploit access points but rather targets clients. Disabling 802.11r (fast roaming) can reduce the exposure to this vulnerability while Riverbed Xirrus make the access point patch available through our support website.

6. **What action should I take on my Wi-Fi network?**
   Applying the appropriate software patches when available is the permanent solution. In the meantime, we recommend you take a few immediate steps to reduce the risk:
   - Turn off TKIP
   - Turn off 802.11r
   - Enable 802.11w

7. **Are other vendors impacted by this vulnerability?**
   Yes. Industry reports indicate that all Wi-Fi vendors are impacted by this vulnerability.

8. **How will I know when the patch for Xirrus APs is available?**
   We will communicate the status of software patches to our customers when available. You can get information through all the means listed below:
   - A customer advisory will be sent to Riverbed Xirrus customers.
   - APs managed by the XMS-Cloud will automatically receive the software patch. APs for customers who have configured specific upgrades windows will receive upgrades during the configured windows.
An announcement will be displayed when you log into XMS-Cloud.
You will be notified of the new software package if you have set up notification on your support community profile.
Announcement will be posted on Xirrus support community

9. Can this vulnerability be easily exploited by an individual with malicious intent?
KRACK is a man in the middle attack and a person executing it will have to have the appropriate equipment and software, and physically be at a given location to access the Wi-Fi signal. This attack cannot be carried out remotely. Riverbed Xirrus takes security threats seriously and recommends that you upgrade the software of your Xirrus APs to latest version as soon as they are released.

10. Does this vulnerability impact the AP, client device or both?
This is a client side vulnerability, meaning, communications from the Wi-Fi device to the AP can be compromised. However, software patches are applicable to both the client and AP infrastructure. We strongly recommend patches be deployed to both when available.

11. Where can I get more information on this vulnerability?
Visit Xirrus support community for additional information on the impact on Xirrus APs and available solution.