Q-CERT Advisory

Key Reinstallation Attacks (KRACK) - Breaking WPA2

Release Date: Oct, 18 2017

Introduction A severe vulnerability has been revealed in WPA2 protocols that used to secure all protected Wi-Fi networks. A potential attacker can exploit this weakness by using Key Reinstallation Attacks called KRACK. This attack can be abused to steal sensitive information such as passwords, email, photos, and any other confidential information passing through the Wi-Fi Network.

Impact An attacker within the wireless access range can exploit the vulnerability and and attack the Wi-Fi access point as well as the wireless client and successfully execute the following :

- Arbitrary packet decryption and injection
- TCP connection hijacking
- HTTP content injection
- Replay of unicast, broadcast, and multicast frames

Affected Systems Any device that supports Wi-Fi, is most likely affected More details for affected systems list could be find in the following list http://www.kb.cert.org/vuls/id/228519

Solution Install updates provided by the vendor for all devices that support WPA2. Most of the vendors have already issued a patch to protect against this attack.

Reporting Q-CERT Team will be available for Emergency Response on 24x7 basis through the following contacts:
Q-CERT Hotline : +974 - 44933408 / +974 - 44995399 Q-CERT
E-Mail: incidents@qcert.org

References For more details find the following references:

- http://www.kb.cert.org/vuls/id/228519
- https://cwe.mitre.org/data/definitions/323.html
- https://www.krackattacks.com/
- https://papers.mathyvanhoef.com/ccs2017.pdf