WiFi Vulnerabilities (#KRACK)

17 Oct 2017.

Severe vulnerabilities have brought all modern secure WiFi networks under serious Threat. Researchers have unearthed flaws in WPA2 protocol implementation in WiFi Clients and Wireless Access points (APs) [1]. It allows replay, decryption or spoof of packets transferred over WiFi networks. Based on the principle of vulnerable technique being used, this has been named KRACK (Key Reinstallation AttaCK). Both 802.1x (EAP) and PSK (password) based networks are affected.

CVE Note:

Following are the CVEs [2] where this vulnerability has been reported:

1. CVE-2017-13077: Reinstallation of the pairwise encryption key (PTK-TK) in the 4-way handshake.
2. CVE-2017-13078: Reinstallation of the group key (GTK) in the 4-way handshake.
3. CVE-2017-13079: Reinstallation of the integrity group key (IGTK) in the 4-way handshake.
4. CVE-2017-13080: Reinstallation of the group key (GTK) in the group key handshake.
5. CVE-2017-13081: Reinstallation of the integrity group key (IGTK) in the group key handshake.
6. CVE-2017-13082: Accepting a retransmitted Fast BSS Transition (FT) Reassociation Request and reinstalling the pairwise encryption key (PTK-TK) while processing it.
7. CVE-2017-13084: Reinstallation of the STK key in the PeerKey handshake.
8. CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake.
9. CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.
10. CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.

Impact:

This vulnerability is because of the underline protocol of WiFi and not specific to any particular product family. Hence anyone using WiFi connection for accessing sensitive information is vulnerable to interception and decryption. Fundamentally, KRACK tricks your device into reinstalling encryption key, meaning the attacker is now able to intercept the victim's communication over WiFi network.

Severity: High

Who all are affected?

Almost all major vendors [3] are affected with this vulnerability. Some of them are shown below:

Cisco, Debian, Fedora, Fortinet, FreeBSD, Google, Intel Corporation, Juniper Networks, Microsoft, Netgear Inc, Red Hat, SUSE Linux, Ubuntu, Check Point, Toshiba, 3com Inc, Apple, Android Open source Project, Cent OS, Dell, D-Link, EMC Corporation, HP, Lenovo, Nokia, Sony, Xiaomi etc.

Immediate work arounds for Critical Information Infrastructure:

1. Use HTTPS only connection to the Server. This will provide additional level of security even if packets are captured by attacker!
2. Users recommended not to use public WiFi.
3. Use wired connection till the vulnerability is appropriately plugged.
4. Use VPN as an additional layer of security between your clients and servers.
5. Need to review BYOD policy for Smart phones in organization (*if any*).

Remedy:

Apply appropriate updates from OEMs on all WiFi devices frequently. E.g. OS of Clients (Systems/Phones) and Firmware of APs. Security updates will assure a key is only installed once and therefore likely to preventing possible attack.

References:

1. https://www.krackattacks.com/
2. https://www.kb.cert.org/vuls/id/228519/
3. https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=228519&SearchOrder=4

Contact:

NCIIPC, Block III, Old JNU Campur, New Dlehi-110067.
Helpline: 1800-11-4430
Email: helpdesk1@nciipc.gov.in; helpdesk2@nciipc.gov.in