CERRT.NG
Computer Emergency
Readiness and Response Team

# WPA2 KEY REINSTALLATION VULNERABILITY

*First published 19th October, 2017*

## 1.0 Overview

It was announced that vulnerabilities have been discovered in widely used WPA2 Wi-Fi security protocol; a protocol which secures majority of Wi-Fi connections. This vulnerabilities can be exploited by an attacker within the range of a target using Key Reinstallation Attack. Using this technique, an attacker can now read and manipulate information formerly presumed to be encrypted.

## 2.0 Impact

a) The vulnerability affects just about any device that uses WPA2 to connect to a Wi-Fi network, which today is about all of them - smart phones, laptops, tablets, routers etc. The most vulnerable so far however appears to be Android devices.

b) An attacker within the wireless communications range of an affected AP and client may exploit these vulnerabilities to conduct attacks that are dependent on the data confidentiality protocol being used. Impacts may include arbitrary packet decryption and injection, TCP connection hijacking or HTTP content injection.

## 3.0 Affected Products

Devices with support for Wi-Fi connectivity using WPA and WPA2 protocols are potentially vulnerable. However a more detailed list of products known to be affected can be read on the following CERT/CC pages:

- https://www.kb.cert.org/vuls/id/228519
- https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=228519&SearchOrder=4

## 4.0 Recommendations

CERRT.NG advises that all Wi-Fi enabled devices should be updated with the latest security updates by the vendor as soon as they are made available and also follow best practice security policies to determine which updates should be applied.

## 5.0 Preventive Measures

- Rather than using Wi-Fi, it's advisable to make use of Ethernet cables where possible and connect directly into the network,.
- Avoid using Wi-Fi that you don't personally administer until all patches and updates have been issued by vendors.
- In best practice, browse the web with an extension such as HTTPS which secures your communication with website.
- Organization can urge their staff to use corporate VPN for any WI-FI connections. While end user can consider using personal VPN for their own personal use.

**NB**: The attack is only feasible if attacker is within range of the Wi-Fi connection. Hence, it is not a remote attack; an attacker in another country cannot hack into a Wi-Fi network in another country.

For further enquiries, please contact CERRT.NG through the following channels:
E-mail: support@cerrt.ng
Phone: ; (+234)-0800998877665544
Web: www.cerrt.ng
Twitter: https://twitter.com/cerrt_ng
Facebook: https://www.facebook.com/cerrtnigeria/

## 6.0 References


- https://securingthehuman.sans.org/blog/2017/10/16/28748/
- https://www.krackattacks.com/
- https://papers.mathyvanhoef.com/ccs2017.pdf
- http://www.kb.cert.org/vuls/id/228519
- https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=228519&SearchOrder=4