ZYXEL
Your Networking Ally

Security advisory for WPA2 “Krack” vulnerabilities (North America Region Service Providers)

2017/10/18

Below are the details for the recently found vulnerabilities of the WiFi Protected Access II (WPA2) security protocol, as identified in US-CERT vulnerability note VU#228519, with vulnerable IDs CVE-2017-13077 through CVE-2017-13082.

Top Highlights:

1. The vulnerabilities are in the Wi-Fi standard itself, and not in individual products or implementations.
2. Attacker has to be physically nearby and within the wireless range to exploit these weaknesses.
3. Zyxel DSL and Ethernet Broadband Gateways are not compromised

What are the vulnerabilities?

These vulnerabilities affect wireless products that connect to WiFi networks in different ways, depending on the role of products as WiFi clients or servers, as described in table 1 below.

Table 1

Type of attack	CVE IDs	Devices impacted
4-way handshake	CVE-2017-13077	WiFi clients
Group-key handshake	CVE-2017-13078 CVE-2017-13079 CVE-2017-13080 CVE-2017-13081	WiFi clients
802.11r Fast-BSS Transition (FT)	CVE-2017-13082	Access points w/802.11r feature

Zyxel DSL and Ethernet Gateways are not compromised

Based on the available information, this Krack vulnerability affects most of the WiFi clients, WiFi AP with repeater and client mode functions, and enterprise style AP with 802.11r function.

Zyxel DSL and Ethernet Gateway products don't support client and repeater mode. 802.11r is not included in shipping firmware. These models (in table 2) sold in North America region are immune from Krack vulnerabilities.

Table 2

DSL CPE	P660HN-51B, P873 series, VSG1432/1435, VMG4325/4380/4381, VMG4825/9823, XMG3512
Ethernet CPE	EMG2306, EMG2926, EMG3425

Affected models and Solution

The Table 3 below contains the affected WiFi repeater/extender models and patch firmware release schedule. Zyxel encourages our customers to update the field units with this patch firmware to mitigate the risk.

Table 3

Product Models	Firmware Availability
WAP6405	1-Nov 2017
WAP6804	6-Nov 2017

Please contact your sales representatives or Zyxel support engineering team (bse@zyxel.com) if you require further information or assistance.

For more information and technical details regarding the vulnerabilities please see below references:

1. US-CERT VU note: https://www.kb.cert.org/vuls/id/228519/
2. Disclosure by Mathy Vanhoef of imec-DistriNet of KU Leuven: https://www.krackattacks.com/