ZYXEL

www.Zyxel.com

Zyxel security advisory for the key management vulnerabilities of WPA2 protocol

20 October 2017

Zyxel is aware of the recently found key management vulnerabilities of the WiFi Protected Access II (WPA2) security protocol, as identified in US-CERT vulnerability note VU#228519 with the vulnerability IDs listed in table 1.

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 CVE-2017-13087 CVE-2017-13088	WiFi clients
802.11r Fast-BSS Transition (FT)	CVE-2017-13082	Access points
Peer-key handshake	CVE-2017-13084 CVE-2017-13086	WiFi clients

It is important to note that an attacker has to be physically nearby and is within the wireless range to exploit these weaknesses.

Please see: https://www.krackattacks.com/#details for more technical information.

How are Zyxel resolving the vulnerabilities?

At Zyxel we treat security as a top priority and we have conducted a thorough investigation and identified a list of vulnerable products within their warranty and support period, as shown in table 2 below. **For products not listed, they are not affected to the attacks either because they are not designed to act as WiFi clients, do not support 802.11r Fast-BSS Transition handshake, or do not support peer-key handshake by default.**

We are now co-working with WiFi chipset vendors to create a solution, and the patch firmware will be available in the next few weeks or even sooner, provided WiFi chipset vendors will release their patches much earlier.

Please refer to table 2 for the detailed release schedule. The hotfix/standard solution firmware will be available for download at Zyxel Support Center.

Table 2

Devices Impacted	Series/Model	Hotfix Availability	Standard Availability
WiFi Clients	NWA1100-NH	31-Dec 2017	Feb 2018
	WAP6405	N/A	1-Nov 2017
	WAP6804	N/A	6-Nov 2017
	WAP6806	16-Nov 2017	Feb 2018
	WRE2206	**17-Nov 2017**	Feb 2018
	WRE6505 v2	16-Nov 2017	Jan 2018
	WRE6606	30-Nov 2017	Feb 2018
	Cam3115	N/A	Feb 2018
	NBG-418n v2	N/A	Dec 2017
	NBG6515	**17-Nov 2017**	Dec 2017
	WAP3205 v3	N/A	Dec 2017
	WRE6505 v1	30-Nov 2017	N/A
	WRE2205 v2	15-Dec 2017	N/A
Access Points	NWA5301-NJ	16-Nov 2017	Feb 2018
	NWA5123-AC	16-Nov 2017	Feb 2018
	WAC6103D-I	16-Nov 2017	Feb 2018

WAC6500 series	16-Nov 2017	Feb 2018

What should I do now to protect myself against the vulnerabilities?

As mentioned previously - It is important to note that an attacker has to be physically nearby and is within the wireless range to exploit these weaknesses. As our business class Access Points support the 802.11r Fast-BSS Transition (FT) handshake, devices supporting this feature are listed in the vulnerability list (table 2). By default, the 802.11r is not enabled in Zyxel Products or Controllers; and the majority of Zyxel customers will not be affected.

For customers who have enabled 802.11r, who are concerned about the security risks, they should disable the 802.11r feature to prevent an attack from taking place. Once the Hotfix has been released, clients wishing to use the 802.11r feature are advised to update as soon as possible to ensure the vulnerability does not affect the security of their network.

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/

Please contact your local service representatives if you require further information or assistance. To report a vulnerability, please contact security@zyxel.com.tw

Zyxel will update this advisory when more information is available.