

Poradnik bezpieczeństwa Zyxel: kluczowe luki protokołu WPA2

W związku z lukami w zabezpieczeniach bezprzewodowego protokołu Wi-Fi Protected Access II (WPA2), które zostały określone w notach US-CERT VU # 228519, CVE-2017-13077, CVE-2017-13082 firma Zyxel postanowiła opisać problem i przedstawić rozwiązania, które pomogą jeszcze skuteczniej chronić sieć bezprzewodową.

Na czym polega problem?

Niebezpieczeństwo dotyczy produktów bezprzewodowych, które łączą się z sieciami Wi-Fi na różne sposoby. W zależności od roli produktu, mogą to być klienci lub serwery, jak opisano w poniższej tabeli:

Tabela 1.

Rodzaj ataku	CVE ID	Dotyczy urządzenia
4-way handshake	CVE-2017-13077	Klient Wi-Fi (wzmacniacze sygnału oraz punkty dostępowe pracujące w trybie wzmacniacza sygnału)
Group-key handshake	CVE-2017-13078 CVE-2017-13079 CVE-2017-13080 CVE-2017-13081	Klient Wi-Fi (wzmacniacze sygnału oraz punkty dostępowe pracujące w trybie wzmacniacza sygnału)
802.11r Fast-BSS Transition (FT)	CVE-2017-13082	Punkt dostępowy z aktywnym IEEE802.11r. Punkty dostępowe Zyxel mają domyślnie nieaktywne IEEE802.11r.

Warto zauważyć, że cyberprzestępca musi znajdować się w pobliżu urządzenia i w zasięgu sieci bezprzewodowych, aby wykorzystać lukę do ataku.¹

Więcej technicznych informacji znajduje się na stronie: <https://www.krackattacks.com/#details>.

Jak ochronić się przed atakami?

Punkty dostępowe klasy biznes obsługują protokół 802.11r Fast-BSS Transition (FT). W związku z tym figurują na liście urządzeń, które są zagrożone atakiem cyberprzestępców (tabela 2). Protokół 802.11r nie jest włączony domyślnie w produktach czy kontrolerach firmy Zyxel. Zatem większość naszych klientów nie musi obawiać się ataków ani wykonywać szczególnych czynności zabezpieczających sieć.

Klienci, którzy włączyli protokół 802.11r, **powinni wyłączyć funkcję 802.11r**, aby zminimalizować ryzyko ataku. Osoby które chcą korzystać z funkcji 802.11r i skorzystały z tzw. hotfix (przygotowanych poprawek), powinny jak najszybciej zaktualizować oprogramowanie, aby mieć pewność, że luka nie stanowi już niebezpieczeństwa dla ich sieci.

Jak Zyxel rozwiązuje problem luk w zabezpieczeniach?

Bezpieczeństwo urządzeń Zyxel i jest dla firmy priorytetem. Dlatego zespół ekspertów Zyxel Communication przeprowadził dokładne badania, dzięki którym udało się zidentyfikować listę produktów narażonych na atak. Wyniki znajdują się w tabeli poniżej. Produkty, które nie są wymienione na poniższej liście, nie są podatne na wspomniane zagrożenie (nie są przeznaczone do działania jako klienci Wi-Fi lub nie obsługują domyślnie protokołu 802.11r Fast-BSS).

Aktualnie zespół Zyxel współpracuje z dostawcami chipsetów Wi-Fi w celu opracowania rozwiązania tego problemu. Aktualizacja będzie dostępna w ciągu kilku najbliższych tygodni.

Szczegółowe informacje o terminach znajdują się w tabeli 2.

¹ <https://www.krackattacks.com/>

Tabela 2

CVE ID	Seria/Model	Dostępność pilna	Standardowa
CVE-2017-13077	NWA1100-NH	31 grudnia 2017	Luty 2018 lub wcześniej
CVE-2017-13078	WAP6405	N/A	1.11. 2017 lub wcześniej
CVE-2017-13079	WAP6804	N/A	6.11. 2017 lub wcześniej
CVE-2017-13080	WAP6806	N/A	Luty 2018 lub wcześniej
CVE-2017-13081	WRE2206	N/A	Luty 2018 lub wcześniej
	WRE6505 v2	N/A	Luty 2018 lub wcześniej
	WRE6606	N/A	Luty 2018 lub wcześniej
	Cam3115	N/A	Luty 2018 lub wcześniej
CVE-2017-13082	Seria NWA1120	16 listopada 2017	Luty 2018 lub wcześniej
	NWA5301-NJ	16 listopada 2017	Luty 2018 lub wcześniej
	Seria NWA5120	16 listopada 2017	Luty 2018 lub wcześniej
	Seria WAC6100	16 listopada 2017	Luty 2018 lub wcześniej
	Seria WAC6500	16 listopada 2017	Luty 2018 lub wcześniej

Więcej informacji i porad technicznych dotyczących problemu znajduje się w poniższych artykułach:

1. US-CERT VU notatka: <https://www.kb.cert.org/vuls/id/228519/>
2. <https://www.krackattacks.com/>

O Zyxel Communications

Zyxel Communications już od prawie 30 lat łączy ludzi koncentrując się na innowacyjności i na klientach. Nasze możliwości adaptacji oraz innowacyjne technologie sieciowe czynią nas liderami komunikacji dla firm telekomunikacyjnych, dostawców usług, firm i użytkowników domowych.

- 1500+ współpracowników na całym świecie
- 100 milionów urządzeń łączących na globalną skalę
- Ponad 700,000 firm pracujących lepiej, dzięki produktom marki Zyxel
- Obecność na 150 światowych rynkach



www.Zyxel.com

Obecnie, Zyxel Communications tworząc sieci przyszłości, uwalnia potencjał i spełnia wymagania nowoczesnych miejsc pracy – wspierając ludzi w biurze, codziennym życiu i w czasie wolnym.

ZYXEL – twój sieciowy sojusznik

Biuro prasowe

Marta Bujakiewicz | Neuron Agencja PR | m.bujakiewicz@neuron.pl | tel. 535 352 423