Domowe rutery pełne dziur

14 lipca 2020

Najpopularniejsze domowe rutery zawierają poważne luki bezpieczeństwa, ostrzegają specjaliści z Instytutu Fraunhofera. Peter Weidenbach i Johannes vom Dorp przeanalizowali pod kątem bezpieczeństwa 127 popularnych domowych ruterów i odkryli, że większość z nich zawiera co najmniej 1 krytyczną dziurę, a w wielu z nich znaleziono setki znanych luk. Jakby tego było mało, średnia liczba krytycznych dziur na ruter wynosiła aż 53, a nawet najbezpieczniejszy z ruterów miał 21 znanych wcześniej luk.

Eksperci przeanalizowali rutery m.in. takich producentów jak Netgear, Linksys, D-Link, ASUS, TP-Link czy Zyxel. Sprawdzali je m.in. pod kątem aktualizacji, wersji systemu operacyjnego, obecności znanych dziur, technik ochrony zastosowanych przez producenta oraz częstotliwości ich aktualizacji, obecności prywatnych kluczy w firmware oraz obecności zakodowanych na twardo haseł dostępowych.

„Podsumowując, nasze analizy wykazały, że nie istnieje ruter bez błędów, a żaden producent nie wykonuje perfekcyjnej roboty pod kątem zabezpieczeń. Producenci muszą włożyć olbrzymi wysiłek w to, by rutery stały się równie bezpieczne jak komputery czy serwery” – mówią autorzy badań.

Co prawda użytkownicy ruterów często popełniają błędy podczas ich konfiguracji, ale to nie one są główną przyczyną, dla której rutery są podatne na ataki. Analiza jasno pokazała, że to producenci tych urządzeń, pomimo tego, że wiedzą o istniejących dziurach, lekceważą swoje obowiązki i dostarczają użytkownikom źle zabezpieczone urządzenia. To lekceważenie klienta najlepiej widać w wersji użytego systemu operacyjnego. Spośród 127 ruterów aż 116 korzystało z Linuksa. Linux może być bardzo bezpiecznym systemem. Problem jednak w tym, że w większości przypadków producenci instalowali w ruterach

przestarzałe wersje oprogramowania, pełne dziur i niedociągnięć. „Większość ruterów korzystała z kernela 2.6, który nie jest utrzymywany od wielu lat [ostatnia wersja tego jądra ukazała się w 2011 roku – red.]. To zaś wiąże się z duża liczbą krytycznych błędów w tych urządzeniach” – napisali badacze.

Kolejny problem to rzadkie aktualizacje firmware’u. Zbyt rzadkie niż być powinny. Nawet jednak odpowiednio częste aktualizacje nie rozwiązują problemów. Okazało się również, że producenci ruterów bardzo rzadko stosują popularne techniki zapobiegania atakom. Bywa nawet tak, że używają powszechnie znanych haseł, których użytkownik nie może zmienić. Jakby jeszcze tego było mało, okazuje się, że w firmware wielu ruterów znajdują się łatwe do pozyskanie prywatne klucze kryptograficzne. To zaś oznacza, że nawet gdy próbujesz zabezpieczyć swój ruter, to nie jest on bezpieczny.

Nie wszyscy producenci ruterów w równej mierze lekceważą klienta. Badacze ocenili, że najlepiej zabezpiecza rutery firma AVM International, chociaż jej produkty również zawierały dziury. Także ASUS i Netgear wyróżniały się pozytywnie na tle innych. Firmy te częściej aktualizowały oprogramowanie swoich urządzeń i wykorzystywały nowsze, wciąż wspierane, wersje jądra Linuksa.
Najgorzej zaś wypadły produkty D-Linka, Linksysa, TP-Linka oraz Zyxela.

Szczegóły analizy można przeczytać w dokumencie „Home router security report 2020” w formacie PDF.

Autorstwo: Mariusz Błoński
Na podstawie: ThreatPost.com
Źródło: KopalniaWiedzy.pl