

BŁĄD SYSTEMU IOS NARAŻA UŻYTKOWNIKÓW NA WYCIEK DANYCH

Błąd występujący w systemie iOS blokuje szyfrowanie ruchu przez VPN-y, co może przyczynić się do wycieku danych użytkowników oraz ujawnić informacje dotyczące ich numerów IP. Problem obejmuje wersję systemu 13.3.1 i późniejsze.

Na błąd wystawione są wszystkie połączenia, które zostały nawiązane przez użytkownika przed połączeniem się z wirtualną siecią prywatną (VPN)- ujawnił zespół Proton VPN, który jako pierwszy poinformował media o problemie.

W wyniku błędu ujawnione mogą zostać dane użytkownika, gdyż nawiązywane połączenia nie są szyfrowane VPN. Luka umożliwia wyciek adresu IP, z jakiego nawiązywana jest łączność, co z kolei prowadzi do ujawnienia lokalizacji danej osoby, a także wywoływanych w ramach połączenia serwerów usług, do których dany użytkownik chce mieć dostęp.

Specjaliści upatrują źródeł problemu w tym, iż Apple nie zaimplementowało w systemie iOS funkcji przerywania wszystkich istniejących połączeń w chwili nawiązania łączności z siecią VPN, by następnie przywrócić je w ramach już zabezpieczonego tunelu ruchu.

Zespół ekspertów Protona zauważa, że większość obecnie nawiązywanych połączeń jest krótkotrwała, co oznacza, że i tak zostaną rozłączone oraz ponownie nawiązane już przez VPN. Niektóre połączenia jednak są długotrwałe i mogą działać bez przerwy od kilku minut do nawet kilku godzin.

Obecnie Proton VPN oraz inni dostawcy tego rodzaju usług nie są zdolni do zapewnienia swoim użytkownikom żadnych możliwości zabezpieczenia się przed działaniem błędu - poinformowali specjaliści. Konieczność usunięcia luki leży po stronie Apple'a, który w konstrukcji systemu iOS nie umożliwia aplikacjom oferującym usługę VPN rozłączania już istniejących połączeń nawiązanych z danego urządzenia.