**Uwaga na zegarki miSafes! Zagrażają bezpieczeństwu Twojego dziecka**

**Nowoczesne zegarki dla dzieci, które umożliwiają rodzicom monitoring miejsca przebywania ich pociech oraz obustronną komunikację, zyskują coraz większą popularność. Kupowane w celu zapewnienia dzieciom bezpieczeństwa, mogą zostać wykorzystane do złych celów.**

Analityk bezpieczeństwa Alan Monie z Pen Test Partners, firmy zajmującej się testowaniem zabezpieczeń sieciowych, odkrył w zegarkach dla dzieci oferowanych przez Misafes poważne luki.

Zegarki miSafes to niedrogie urządzenia (kosztują ok. 10 funtów) wyposażone w GPS oraz modem GSM. Po zainstalowaniu w nich karty SIM można rozmawiać z dzieckiem, wysyłać mu wiadomości, sprawdzać gdzie aktualnie przebywa oraz otrzymać wezwania SOS.

W przypadku większości dostępnych na rynku zegarków o podobnej funkcjonalności, przejęcie nad nimi kontroli wymaga fizycznego dostępu do urządzenia, w celu poznania numeru IMEI. Natomiast z zegarkami miSafes jest inaczej. Monie odkrył, że w przypadku tych urządzeń, aby włamać się do zegarka wystarczy zdalny dostęp za pośrednictwem sieci komórkowej.

Luka została wykryta za pomocą Burpa – ogólnodostępnego narzędzia do testowania bezpieczeństwa aplikacji internetowych – który pozwala m.in. kontrolować i analizować ruch pomiędzy aplikacją miSafes a serwerem pośredniczącym (proxy) w komunikacji z zegarkami. Okazało się, że transmisja danych nie jest szyfrowana i łatwo można podmienić informacje (np. numer telefoniczny umieszczonej w zegarku karty sim, hasło i inne) na spreparowane.

Taka metoda ataku pozwala przechwycić numer IMEI (czyli dokładnie wiemy, do którego zegarka zyskaliśmy nieautoryzowany dostęp) oraz poznać położenie wszystkich zegarków zalogowanych do sieci komórkowej. W połączeniu z fałszowaniem identyfikatora rodzica, metoda staje się poważnym zagrożeniem dla bezpieczeństwa dzieci.

Metodą tą Monie zyskał dostęp do aktualizowanej w czasie rzeczywistym lokalizacji wszystkich dzieci posiadających zegarek miSafes. Mógł również zestawić jednokierunkowe połączenie głosowe, pozwalające nasłuchiwać, co się dzieje w otoczeniu dziecka oraz wysłać mu wiadomość audio. Co gorsze, mógł się podszyć pod rodzica wysyłającego do swojego dziecka wiadomość tekstową.

Więcej szczegółów nt. ataku dostępnych jest na blogu Moniego pod adresem:

https://www.pentestpartners.com/security-blog/tracking-and-snooping-on-a-million-kids/

Zarówno autor ataku, jak i zainteresowane media (w tym BBC) skontaktowali się z producentem z prośbą o komentarz. Do tej pory Misafes nie udzielił odpowiedzi.

„Produkty, które będą w użytkowaniu dzieci powinny w szczególny sposób być zabezpieczone. Przed zakupem nowoczesnych gadżetów powinniśmy dokładnie sprawdzić, czy nie narażamy najmłodszych na niebezpieczeństwo” komentuje Dariusz Woźniak, inżynier techniczny Bitdefender z firmy Marken.