**Analitycy znaleźli potencjalnie zagrażającą życiu usterkę w defibrylatorach Medtronic Cardio**

**Agencja ds. Cyberbezpieczeństwa i Zabezpieczenia Infrastruktury (CISA) amerykańskiego Departamentu Bezpieczeństwa Narodowego wydała pilne zawiadomienie dotyczące defibrylatorów serca firmy Medtronic. Analitycy wykryli w warstwie sprzętowej urządzenia krytyczne luki, które, w przypadku wykorzystania, mogły zagrozić życiu pacjenta.**

O ile dawniej wprowadzenie modyfikacji w defibrylatorze wymagało otwarcia ciała pacjenta, to współczesne – bardziej zaawansowane – urządzenia mogą być obsługiwane zdalnie. Stwarza to jednak ogromne problemy w przypadku, gdy sprzęt jest wadliwy.

Urządzenie, o którym mowa, daje możliwość bezprzewodowego programowania, kalibrowania i nadzorowania. Według analityków, zastrzeżony protokół komunikacyjny firmy Medtronic, wykorzystywany w komunikacji z wszczepionymi urządzeniami, nie jest szyfrowany, co pozwala na ataki typu man-in-the-middle (podsłuchiwanie, filtrowanie danych). Protokół nie zawiera również uwierzytelniania, co oznacza, że zmotywowany napastnik może próbować włamać się do implantu za pomocą specjalnie przystosowanego sterownika.

Z porad CISA:

„Pomyślne wykorzystanie tych luk może pozwolić atakującemu, w którego pobliżu znajduje się pacjent z wszczepionym urządzeniem, na zakłócanie, generowanie, modyfikowanie lub przechwytywanie ruchu odbywającego się przez kanał radiowy z wykorzystaniem zastrzeżonego systemu telemetrycznego Conexux firmy Medtronic, potencjalnie wpływając na funkcjonowanie urządzenia i/lub uzyskując dostęp do przesyłanych wrażliwych danych... Skutkiem udanego wykorzystania tych luk może być odczyt i zapis dowolnego obszaru pamięci wewnętrznej implantowanego aparatu, a tym samym celowy wpływ na realizację wybranej funkcji”.

Ponieważ zadaniem defibrylatora jest zapewnienie prawidłowej akcji serca, więc każda ingerencja w jego zachowanie może zagrażać życiu pacjenta. CISA przedstawiła pacjentom, w których klatkach piersiowych znajdują się urządzenia Medtronic.

**Marken Systemy Antywirusowe - przedstawiciel marki Bitdefender w Polsce (https://bitdefender.pl) , daje użytkownikom następującą listę koniecznych do przestrzegania środków ostrożności**:

*⦁ Nie podłączaj nieuwierzytelnionych urządzeń do monitorów domowych i programatorów przez porty USB lub inne łącza fizyczne.*

*⦁ Korzystaj wyłącznie z programatorów dedykowanych dla wszczepionego urządzenia i zezwalaj na interakcję z nimi jedynie w pozostających pod fizyczną kontrolą szpitalach i klinikach.*

*⦁ Używaj monitorów domowych jedynie w środowisku prywatnym, takim jak dom, mieszkanie lub inna kontrolowana fizycznie przestrzeń.*

*⦁ Utrzymuj stałą kontrolę fizyczną nad monitorami domowymi i programatorami.*

*⦁ Używaj wyłącznie monitorów domowych, programatorów i implantów pochodzących bezpośrednio od swojej jednostki opieki zdrowotnej lub przedstawiciela firmy Medtronic, co zapewni integralność systemu.*

*⦁ Wszelkie spostrzeżenia dotyczące zachowania tych urządzeń zgłaszaj swojemu lekarzowi lub przedstawicielowi firmy Medtronic.*

W oświadczeniu dla Ars Technica, Medtronic zbagatelizował zarzuty, że luki w jego sprzęcie są poważne, ale też im nie zaprzeczał.

Przedstawiciel firmy, Ryan Mathre, informuje media, że ryzyko wykorzystania luk w zabezpieczeniach jest niskie, ponieważ „nieautoryzowany użytkownik potrzebowałby kompleksowej i specjalistycznej wiedzy na temat urządzeń medycznych, telemetrii bezprzewodowej i elektrofizjologii, aby wykorzystać te luki i zaszkodzić pacjentowi”.

W każdym razie, powiedział Mathre, Medtronic pracuje nad aktualizacją sprzętu, którą planuje wprowadzić jeszcze w tym roku.