"BLEEDING TOOTH". PODATNOŚĆ BLUETOOTH ZAGROŻENIEM DLA UŻYTKOWNIKÓW LINUXA

Intel i Google ostrzegają przed poważną podatnością bezpieczeństwa technologii Bluetooth, która występuje w systemie Linux. Luka umożliwia potencjalnym atakującym zdalne wykonanie kodu na urządzeniu znajdującym się w zasięgu sygnału Bluetooth.

Zdaniem ekspertów z obu firm, wykryta podatność może być wykorzystana m.in. do nieuprawnionego pozyskiwania danych z atakowanych urządzeń.

Podatność wykryta przez specjalistów została ochrzczona mianem "Bleeding Tooth" (krwawiący ząb). Zdaniem inżyniera Google'a Andy'ego Nguyena wykorzystanie luki przez hakerów nie wymaga od nich żadnej interakcji z atakowanym urządzeniem. Każda osoba znajdująca się w odpowiedniej odległości od komputera-ofiary może wykonać na nim zdalnie kod, który umożliwia zdobycie przywilejów administratora oraz pozyskanie np. poufnych danych.

Luka "Bleeding Tooth" znajduje się w module oprogramowania BlueZ, który służy do implementacji kluczowych protokołów technologii Bluetooth w systemie Linux. Poza komputerami działającymi w oparciu o ten system, moduł BlueZ wykorzystywany jest również przez szeroko dostępne na rynku urządzenia internetu rzeczy - zarówno te z segmentu konsumenckiego, jak i te stosowane w przemyśle.

BlueZ współpracuje z systemem Linux w wersji 2.4.6 oraz wszystkimi późniejszymi.

Nguyen cytowany przez serwis Ars Technica twierdzi, że odkrycie podatności "Bleeding Tooth" zostało dokonane przypadkowo podczas innych badań z zakresu cyberbezpieczeństwa. Dotyczyły one innej luki znanej jako "BlueBorne", pozwalającej cyberprzestępcom na wysyłanie dowolnemu urządzeniu poleceń, które są wykonywane zdalnie i nie muszą zostać uruchomione przez użytkownika klikającego np. w złośliwy link lub podłączającego swoje urządzenie do innego, zainfekowanego przez hakerów. Do ataku z wykorzystaniem "BlueBorne" według ekspertów wystarczy jedynie włączona komunikacja Bluetooth u ofiary.

Intel, który ma bardzo duży wkład w rozwój modułu BlueZ (oprogramowanie to tworzone jest w ramach projektu open-source), twierdzi, iż najlepszą metodą zabezpieczenia się przed działaniem nowowykrytej podatności "Bleeding Tooth" jest aktualizacja jądra systemu Linux do wersji 5.9.