Nie do naprawienia dziura w chipsetach Intela

15 marca 2020

W chipsetach Intela używanych od ostatnich pięciu lat istnieje dziura, która pozwala cyberprzestępcom na ominięcie zabezpieczeń i zainstalowanie szkodliwego kodu takiego jak keyloggery. Co gorsza, luki nie można całkowicie załatać.

Jak poinformowała firma Positive Technologies, błąd jest zakodowany w pamięci ROM, z której komputer pobiera dane podczas startu. Występuje on na poziomie sprzętowym, nie można go usunąć. Pozwala za to na przeprowadzenie niezauważalnego ataku, na który narażone są miliony urządzeń.

Na szczęście możliwości napastnika są dość mocno ograniczone. Przeprowadzenie skutecznego ataku wymaga bowiem bezpośredniego dostępu do komputera lub sieci lokalnej, w której się on znajduje. Ponadto przeszkodę stanowi też klucz kryptograficzny wewnątrz programowalnej pamięci OTP (one-time programable). Jednak jednostka inicjująca klucz szyfrujący jest również podatna na atak.

Problem jest poważny, szczególnie zaś dotyczy przedsiębiorstw, które mogą być przez niego narażone na szpiegostwo przemysłowe. „Jako, że błąd w ROM pozwala na przejęcie kontroli zanim jeszcze zabezpieczony zostanie sprzętowy mechanizm generowania klucza kryptograficznego i jako, że błędu tego nie można naprawić, sądzimy, że zdobycie tego klucza jest tylko kwestią czasu” – stwierdzili przedstawiciele Positive Technologies.

Błąd występuję w chipsetach Intela sprzedawanych w przeciągu ostatnich 5 lat. Wyjątkiem są najnowsze chipsety 10. generacji, w której został on poprawiony.

Intel dowiedział się o dziurze jesienią ubiegłego roku. Przed

kilkoma dniami firma opublikowała poprawkę, która rozwiązuje problem. Firma przyznaje, że programowe naprawienie dziury jest niemożliwe. Dlatego też poprawka działa poprzez poddanie kwarantannie wszystkich potencjalnych celów ataku.

Dziura znajduje się w Converged Security Management Engine (CSME), który jest odpowiedzialny za bezpieczeństwo firmware'u we wszystkich maszynach wykorzystujących sprzęt Intela.

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