Cyberdefence 24

aut. Szymon Palczewski 07.04.2020

AMERYKAŃSKIE MIASTA Z KRYTYCZNYMI LUKAMI W OPROGRAMOWANIU

Krytyczne luki w oprogramowaniu wykorzystywanym przez podmioty publiczne w amerykańskich miastach umożliwiały hakerom przeprowadzenie złośliwych operacji, wymierzonych między innymi w bazy danych. Podatność została wykryta zanim przeprowadzono ukierunkowany cyberatak.

Quentin Rhoads-Herrera, specjalista firmy Critical Start, odkrył groźne luki, gdy jedna z miejskich władz w Stanach Zjednoczonych podała mu kod źródłowy oprogramowania, którego miasto używa do zarządzania umowami i śledzenia projektów infrastrukturalnych – informuje serwis CyberScoop.

Ekspert dogłębnie zbadał oprogramowanie i wykrył ponad 12 wcześniej nieujawnionych luk, które hakerzy mogli wykorzystać na przykład do manipulowania danymi. Dwa inne miasta również korzystały z wadliwego oprogramowania.

Jak wskazuje CyberScoop, produkt, znany jako CIPAce, był używany przez organizacje sektora publicznego i prywatnego do zbierania faktur oraz zarządzania umowami, a także budżetami. „Jeśli napastnik wykorzysta to miasto, może łatwo zobaczyć, że inne też z tego korzystają i zaatakować je przy użyciu tych samych metod" – podkreślił Quentin Rhoads-Herrera dla CyberScoop. Dodał, że oczywiście podjął próbę skontaktowania się z pozostałymi miastami, które korzystają z wadliwego oprogramowania.

Równocześnie ekspert podkreślił, że nie zauważył żadnych złośliwych operacji hakerskich wykorzystujących luki w oprogramowaniu CIPPlanner. Wyjaśnił jednak, że wskazane luki mogą być dużym problemem nie tylko dla administracji publicznej, ale i każdej innej organizacji.

Wayne Xie, dyrektor CIPPlanner, w rozmowie z CyberScoop wskazał, że jego firma nieustannie ulepsza swoje produkty, aby były bezpieczniejsze. „Kontynuujemy aktualizację oprogramowania i przeprowadzamy testy penetracyjne" – podkreślił. Specjaliści są jednak zdania, że niektóre elementy CIPPlanner nie były aktualizowane od lat.

Luki wykryte przez Critical Start mogły pozwolić hakerowi na ujawnienie danych z wewnętrznych baz lub wstrzyknięcie złośliwego oprogramowania w celu manipulowania informacjami.

Quentin Rhoads-Herrera na łamach CyberScoop wskazał, że władze publiczne bardzo zaangażowały się w próby zabezpieczenia infrastruktury. To proaktywne podejście do bezpieczeństwa jest tym ważniejsze, że ludzie w całym kraju pracują zdalnie podczas pandemii koronawirusa.