Hakerzy włamali się do 12 norweskich ministerstw

28 lipca 2023

Niezidentyfikowani hakerzy wykorzystali lukę dnia zerowego w oprogramowaniu Ivanti do scentralizowanego zarządzania firmowymi urządzeniami mobilnymi i z powodzeniem przeprowadzili cyberatak na zasoby dwunastu norweskich agencji rządowych. Twórcy oprogramowania naprawili błąd, ale zasoby kilku tysięcy innych organizacji mogą pozostać zagrożone.

Norweska Organizacja ds. Bezpieczeństwa i Usług (DSS) poinformowała, że atak zhakował platformy informatyczne wykorzystywane przez dwanaście ministerstw. Ich nazw nie podano, ale resort dodał, że incydent nie wpłynął na zasoby kancelarii premiera, a także ministerstw obrony, sprawiedliwości i spraw zagranicznych. DSS poinformowało również, że cyberatak był możliwy z powodu „nieznanej wcześniej luki w oprogramowaniu jednego z dostawców". Norweski Urząd ds. Bezpieczeństwa Narodowego (NSM) dodał następnie, że jest to luka w Ivanti Endpoint Manager Mobile (EPMM, wcześniej znana jako MobileIron Core).

Ivanti EPMM umożliwia autoryzowanym użytkownikom i urządzeniom dostęp do sieci korporacyjnych i rządowych. Luka CVE-2023-35078 umożliwia ominięcie procedury uwierzytelniania i dotyczy wszystkich obsługiwanych i nieobsługiwanych wersji programu wdrożonych przed jej wykryciem. Po wykorzystaniu luka umożliwia każdemu zdalny dostęp do danych osobowych użytkowników urządzeń mobilnych (nazwiska, numery telefonów i inne dane), a także wprowadzanie zmian na zhakowanym serwerze. Amerykańska Agencja ds. Cyberbezpieczeństwa i Ochrony Infrastruktury (CISA) wyjaśniła również, że luka umożliwia atakującym tworzenie kont z uprawnieniami administracyjnymi w zaatakowanych systemach i wprowadzanie zmian w platformie.

Dyrektor ds. bezpieczeństwa Ivanti, Daniel Spicer, powiedział, że firma niezwłocznie wydała aktualizacje oprogramowania, aby naprawić lukę, i skontaktowała się z klientami, aby pomóc im zainstalować aktualizację. Zapewnił również, że firma „potwierdziła swoje zaangażowanie w dostarczanie i wspieranie bezpiecznych produktów poprzez stosowanie odpowiedzialnych protokołów ujawniania informacji". Jednak firma Ivanti ukryła szczegółowe informacje o luce, która została oceniona 10 na 10, za „paywallem" – dostęp do bazy wiedzy wymaga konta klienta, jak określono w zasobie TechCrunch.

Prawdziwa skala incydentu jest nadal nieznana. Według serwisu wyszukiwania Shodan w Internecie dostępnych jest obecnie ponad 2900 portali Ivanti MobileIron, z których większość należy do klientów amerykańskich.

Autorstwo: tallinn
Źródło: ZmianyNaZiemi.pl