aut. Andrzej Kozłowski 08.01.2021

TAJEMNICE NISSANA W SIECI

Kod źródłowy mobilnych aplikacji oraz wewnętrznych narzędzi używanych przez Nissan North America do projektowania i produkcji samochodów wyciekły do sieci. Przyczyną był źle skonfigurowany jeden z serwerów GIT.

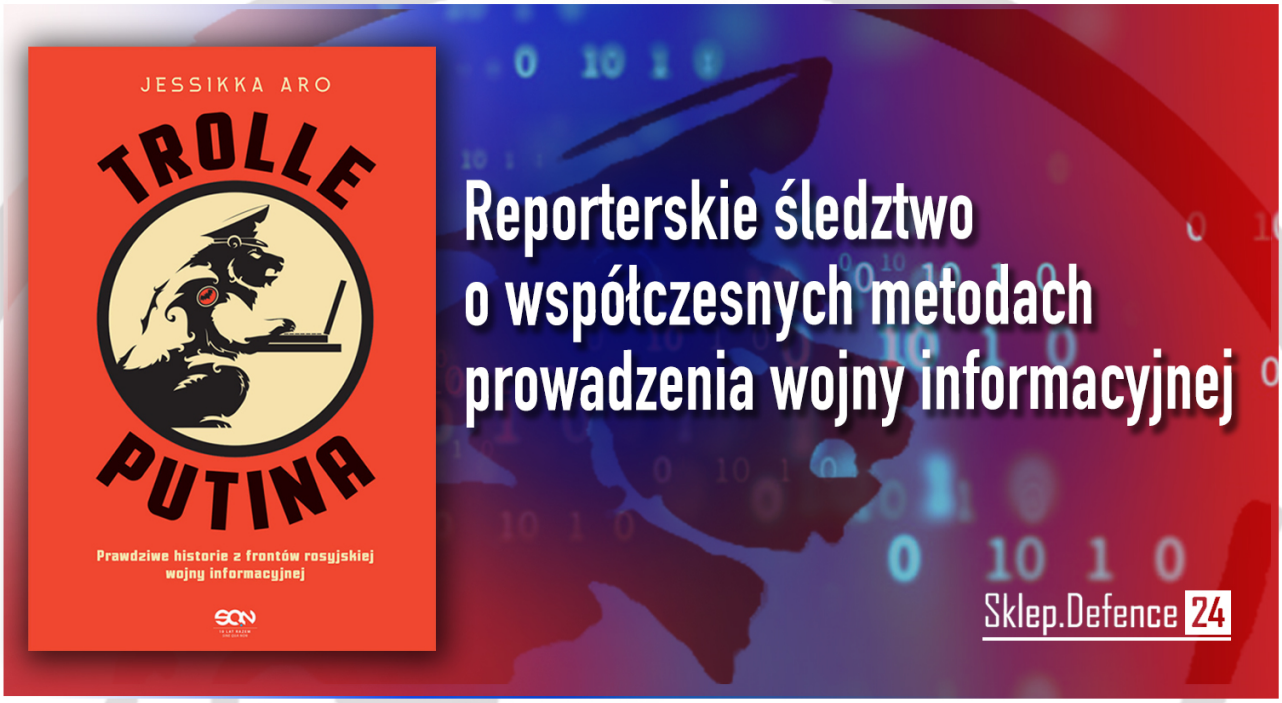
Nissan wszczął śledztwo w sprawie ujawnienia poufnych informacji i kodu źródłowego. Rzecznik prasowy koncernu poinformował, że incydent jest traktowany bardzo poważnie. Informacje, które wyciekły dotyczą m.in. systemów diagnostycznych, narzędzi serwisowania, narzędzi do pozyskiwania i utrzymywania klientów, danych o sprzedaży i narzędzi do badania rynku czy do łączenia się z pojazdami.

Według wstępnych informacji wyciek danych pochodzi z serwera GIT, który został źle zabezpieczony. Nie zmieniono standardowych danych loginów i haseł, co jest błędem charakterystycznym dla początkujących osób stawiających swoje pierwsze kroki w konfiguracji sieciowej. Po tym jak wykryto wyciek, serwer został natychmiast odłączony od sieci. Dane te, co nie powinno nikogo dziwić, krążą już po różnorodnych forach w Internecie.

Czytaj też: Wyciek danych z serwisów randkowych. Tajemnice użytkowników krążą w sieci

Źle skonfigurowane serwery są często przyczyną wycieków danych. Doprowadziły one do ujawnienia informacji z portali randkowych, hoteli czy nawet jednostek medycznych. Nissan, a dokładnie jego kanadyjska odnoga, padł już wcześniej ofiarą hakerów. W 2017 roku roku w wycieku danych ucierpiało 17 milionów osób.

Czytaj też: Wyciek danych z popularnej platformy e-commerce. Zawinili pracownicy?



[Oferta sklepu Defence24]