aut. Szymon Palczewski 02.07.2020

CHIŃSKIE SYSTEMY MONITORINGU ZAGROŻENIEM DLA PAŃSTWA

Kamery chińskich producentów zawierają luki, które umożliwiają przesyłanie danych na serwery znajdujące się w Chinach – wynika z analizy przeprowadzonej przez litewskie Narodowe Centrum Bezpieczeństwa Cybernetycznego (NCSC). Nie jest to jedyna podatność, jaka została wykryta przez specjalistów w chińskim sprzęcie.

NCSC, działające przy Ministerstwie Obrony Narodowej, przeprowadziło ocenę kamer monitorujących chińskich producentów Hikvision i Dahua. Analiza została wykonana z myślą o potrzebach państwowych i medialnych instytucji w zakresie cyberbezpieczeństwa. „Dochodzenie zostało przeprowadzone niezależnie i bez udziału producenta" – czytamy w treści analizy. Obecnie ze sprzętu wspominanych marek korzysta 57 instytucji w całym kraju.

Producent systemu nadzoru wideo Hangzhou Hikvision Digital Technology Co. to chińska firma założona w 2001 roku, zatrudniająca 26 000 pracowników. W samym 2020 roku koncern wprowadził na rynek ponad 300 nowych produktów.

„Rozwiązania Hikvision są skierowane do szerokiej grupy odbiorców – od sektora przemysłowego po sprzęt domowy" – wskazuje analiza. Produkty Hikvision stanowią 22% światowych systemów nadzoru wideo i są eksportowane do ponad 150 krajów.

Przedmiotem badania objęte zostały również produkty firmy Zhejiang Dahua Technology Co. Marka została założona w 2001 roku i specjalizuje się w technologii nadzoru wideo. Obecnie korporacja zatrudnia 13 000 pracowników oraz dostarcza produkty do ponad 180 krajów.

Firma stanęła w ogniu krytyki, gdy okazało się, że jej produkty nie zapewniają odpowiedniego poziomu cyberbezpieczeństwa. W 2017 roku specjaliści odkryli luki w oprogramowaniu produktów Dahua, które umożliwiały przesyłanie danych do Chin.

„Za pomocą przeglądarki internetowej luka umożliwiała nieupoważnionym osobom zdalne pobranie bazy danych na temat nazw użytkowników i haseł do urządzenia, a następnie dostęp do elementów sterowania kamerą" – czytamy w analizie.

Na skutek incydentu władze firmy podjęły decyzję o wydaniu aktualizacji oprogramowania, dzięki której udało się usunąć 11 luk w zabezpieczeniach. Eksperci wskazują, że było to jedynie pozorne działanie, ponieważ podatność umożliwiająca przesyłanie danych nadal występowała po wydaniu „łatek".

Analiza kamer monitorujących Hikvision i Dahua wykazała, że wykorzystują one rozwiązania programowe opracowane w latach 2012–2015 i zawierają luki w zabezpieczeniach. Podatności dotyczą głównie zagrożenia związanego ze zdalnym przechwytywaniem informacji z urządzeń, a także

możliwością przeprowadzenia skutecznego ataku typu DDoS.

„Warto zaznaczyć, że na badanych urządzeniach znaleziono rozwiązania bezpieczeństwa, które pozwalają wyeliminować problem nieautoryzowanego dostępu, lecz nie były one jednak aktywne w standardowej konfiguracji" – stwierdzono w analizie. Co więcej, w urządzeniach nie znaleziono funkcji automatycznej aktualizacji. Czynność tą należy samodzielnie pobrać i wykonać ręcznie.