NSA stoi za backdoorami w urządzeniach sieciowych?

29 grudnia 2015

Ledwie w internecie rozniosła się informacja o znalezieniu dwóch tylnych drzwi w urządzeniach sieciowych firmy Juniper Networks, a już wskazano prawdopodobnego winnego ich istnienia. Ralf-Philipp Weinmann, niemiecki ekspert ds. bezpieczeństwa komputerowego, twierdzi, że za backdoorami stoi NSA.

Jeden z dwóch backdoorów pozwala na odszyfrowanie ruchu przechodzącego przez urządzenia Junipera. Znajduje się on w ScreenOS 6.2.0r12 i innych wersjach firmware'u. Zdaniem Weinmanna to sposób, w jaki działa backdoor zdradza, że stoi za nim NAS. ScreenOS wykorzystuje, zatwierdzony przez instytucje rządowe, algorytm Dual_EC do generowania liczb losowych używanych do szyfrowania. Podejrzenia co do działalności tego algorytmu pojawiły się już w 2007 roku, a w roku 2013 Edward Snowden ujawnił projekt BULLRUN, w ramach którego NSA dążyła do celowego osłabienia narzędzi i standardów przemysłowych. Skupiała się przy tym szczególnie na Dual_EC. Następnie w latach 2014 i 2015 eksperci dowodzili, że celowe osłabienie Dual_EC przez NSA może zostać wykorzystane do umieszczenia tylnych drzwi i odszyfrowania danych.

W 2013 roku Juniper zapewnił, że Dual_EC nie jest podstawowym generatorem liczb losowych w jego urządzeniach. Ponadto firma dodała, że używa takiej wersji Dual_EC, która została zmieniona względem standardowej. To powinno zabezpieczyć przed backdoorem.

Teraz okazało się, ze od 2012 roku używana jest standardowa edycja Dual_EC. Zdaniem Weinmanna, ktoś bez zgody Junipera dokonał w oprogramowaniu takich zmian, by NSA mogła wykorzystać tylne drzwi. Niewykluczone, że dało to agencji

dostęp do wszelkich danych przesyłanych za pośrednictwem urządzeń Junipera.

Autorstwo: Mariusz Błoński
Na podstawie: Enterprise-Security-Today.com
Źródło: KopalniaWiedzy.pl