

KLIENCI RBS ZAGROŻENI CYBERATAKIEM

Klienci Royal Bank of Scotland (RBS) zostali narażeni na cyberataki, po tym jak zainstalowali oprogramowanie, które w teorii miało zagwarantować im bezpieczeństwo. Problem w tym, że zawierało ono krytyczną lukę.

Na początku roku RBS włączyło do swojej oferty dla klientów biznesowych darmowy produkt nazwany „Thor Foresight”. Narzędzie zostało okrzyknięte rewolucyjnym postępowaniem w ochronie przed zagrożeniami płynącymi z cyberprzestrzeni. Okazało się, że sytuacja wygląda jednak inaczej. Naukowcy odkryli błąd, który narażał klientów na zagrożenie. Według doniesień BBC aplikacja z błędem miało używać prawie 50 tys. użytkowników. Dokładne dane nie są jednak znane, ponieważ RBC nie ujawnia tego typu informacji. RBC poinformowało, że błąd został już naprawiony.

Błąd miał zostać odkryty przez zespół zewnętrznych pentesterów, którzy utrzymują, że był on bardzo poważny. Jeden z badaczy Ken Munro powiedział BBC, że uzyskanie kontroli nad sprzętem ofiary była banalnie prosta. Atakujący mogli przejąć całkowitą kontrolę nad emailami, internetową historią i detalami banku. Badacz wyjaśnia, że w tym celu musieli przejąć przesyłane przez użytkownika dane. Jak tłumaczył jest to jednak bardzo proste, ponieważ wielu użytkowników podłącza się do niestrzeżonych punktów wi-fi.

Thor Foresight jest programem odpowiadającym za bezpieczeństwo, dlatego tak ważne jest, żeby utrzymywało standardy najwyższej jakości. Działanie tego oprogramowania można porównać do filtra, którego zadaniem jest znalezienie i zatrzymanie cyberataków, które próbują ukraść informacje lub też zainfekować sprzęty.

Morten Kjaersgaard odpowiedzialny za bezpieczeństwo powiedział, że jest ono traktowane priorytetowo. Dodał, że luka została załataną w przeciągu 4 dni na 97 % dotkniętych maszynach. Błąd funkcjonował przez 3 dni.