**Gra FORTNITE narażona na ataki hakerskie!**

**Badacze firmy Check Point® Software Technologies Ltd. ogłosili dziś szczegóły podatności, które mogłyby dotknąć każdego gracza ogromnie popularnej gry online, Fortnite. W Fortnite gra prawie 80 milionów graczy na całym świecie, a sama gra jest popularna na wszystkich platformach, Android, iOS, Windows PC, a także na konsolach takich jak Xbox One czy PlayStation 4. Jest ona źródłem zainteresowania nie tylko wśród graczy-amatorów, ale także wśród profesjonalistów, którzy streamują swoje sesje online oraz entuzjastów e-sportów.**

Jeżeli podatność zostałaby wykorzystana, dałaby ona atakującemu pełny dostęp do konta użytkownika, do jego danych osobistych, a także pozwoliłaby na zakup wirtualnej waluty obowiązującej w grze korzystając z karty płatniczej gracza. Podatność pozwoliłaby także na poważne naruszenie prywatności: haker mógłby podsłuchiwać rozmowy w grze oraz wszystkie dźwięki otoczenia w domu ofiary czy innej lokalizacji gry. Jak dotąd gracze Fortnite byli atakowani za pomocą fałszywych stron internetowych, obiecujących generowanie ‘V-Bucków’ (waluty obowiązującej w grze, ale ta podatność mogła zostać wykorzystana bez podania przez gracza danych logowania.

Badacze opisali proces, w którym atakujący mógł uzyskać dostęp do konta użytkownika poprzez wykorzystanie podatności w procesie logowania. Na skutek trzech defektów znalezionych w infrastrukturze sieciowej Epic Games, badacze byli w stanie zademonstrować proces uwierzytelniania oparty na tokenie w połączeniu z systemami Single-Sign-On (SSO) takimi jak Facebook, Google i Xbox, za pomocą którego było możliwe przechwycenie danych logowania i przejęcie konta użytkownika.

Aby paść ofiarą tego ataku, gracz musi jedynie kliknąć na spreparowany link phishingowy, dla uśpienia czujności pochodzący z domeny Epic Games, lecz wysłany przez atakującego. Po kliknięciu w niego, token uwierzytelniający użytkownika mógł zostać przechwycony przez atakującego i to bez wpisywania danych logowania przez użytkownika. Według badaczy firmy Check Point, ta podatność pochodziła z defektów znalezionych w dwóch subdomenach Epic Games, które były podatne na złośliwe przekierowania, co pozwalało hakerom na przechwycenie tokenów uwierzytelniających korzystając ze skompromitowanej subdomeny.

“Fortnite jest jedną z najpopularniejszych gier, w które grają głównie dzieci. Te defekty zabezpieczeń mogły doprowadzić do ogromnych naruszeń prywatności” - powiedział Oded Vanunu, szef działu badań podatności produktów firmy Check Point. - “Wraz z podatnościami, które ostatnio znaleźliśmy w systemach firmy produkującej drony [DJI](https://research.checkpoint.com/dji-drone-vulnerability/), pokazują one jak bardzo podatne na ataki są aplikacje w chmurze. Platformy tego typu stają się coraz częstszym celem hakerów, ponieważ przechowują ogromne ilości wrażliwych danych klientów. Wymuszenie dwustopniowego uwierzytelniania mogłoby zapobiec podatnościom na przejęcie kont.”

Check Point poinformowało Epic Games o podatności, która została już naprawiona. Check Point i Epic Games doradzają wszystkim użytkownikom zachować czujność w każdej sytuacji wymieniania informacji cyfrowych i stosować się do dobrych praktyk dotyczących cyberbezpieczeństwa przy komunikowaniu się z innymi użytkownikami online. Użytkownicy powinni również zawsze poddawać w wątpliwość uczciwość linków, które są udostępniane na forach i stronach internetowych.

Organizacje powinny przeprowadzać regularne i szczegółowe testy zabezpieczeń swojej infrastruktury IT, żeby upewnić się, że nie pozostawiono nieużywanych i przestarzałych subdomen, stron i punktów dostępu online.

W celu zminimalizowania ryzyka stania się ofiarą ataku z wykorzystaniem podatności takich jak opisana powyżej, użytkownicy powinni włączyć dwustopniowe uwierzytelnianie, które wymaga podania przez użytkownika kodu bezpieczeństwa wysyłanego na adres email przy każdej próbie logowania z nowego urządzenia. Ważne również jest, żeby rodzice uświadamiali dzieci w kwestii niebezpieczeństw internetowych i ostrzegli je przed hakerami, którzy zrobią wszystko w celu pozyskania danych osobowych i płatniczych, które mogą być przechowywane na koncie gracza.