**Ponad 300 mln użytkowników EA Origin zagrożonych!**

**Zespoły badawcze firmy Check Point oraz CyberInt wykryły poważny „łańcuch podatności” w platformie Origin, pozwalający hakerom na przejęcie kont EA Games oraz kradzież tożsamości nawet 300 milionów graczy na całym świecie! Winowajcą okazały się źle zabezpieczone tokeny autoryzacyjne.**

W ciągu ostatnich kilku tygodni, Check Point Research połączyło siły z CyberInt celem identyfikacji zestawu podatności, które wykorzystane, mogłyby doprowadzić do przejęcia milionów kont graczy na platformie drugiego na świecie co do wielkości producenta gier komputerowych, EA Games. Atakujący mogli potencjalnie uzyskać dostęp do numerów kart kredytowych użytkowników, a także kupować cyfrową walutę dostępną w grach na ich koszt.

CyberInt i Check Point natychmiast poinformowały EA Games o tych lukach bezpieczeństwa i wspólnie wsparły EA w ich naprawieniu, żeby zabezpieczyć graczy.

Podobnie jak w przypadku wcześniejszych odkryć firmy Check Point Research dotyczących innej ogromnie popularnej gry online, [Fortnite](https://research.checkpoint.com/hacking-fortnite/), podatności znalezione na platformie EA nie wymagały przekazania przez użytkownika żadnych danych. Zostały one oparte na wykorzystaniu tokenów autoryzacyjnych wraz z techniką oAuth SSO (Single Sign-On) i mechanizmem TRUST, który jest wbudowany w proces logowania użytkowników.

EA Games wykorzystuje chmurę Microsoft Azure do hostowania kilku domen takich jak ea.com i origin.com w celu zapewnienia globalnego dostępu do różnych usług dla graczy - takich jak tworzenie nowych kont, łączenie się z siecią społecznościową Origin i kupowanie gier w sklepie internetowym EA.

**Jak mógł przebiegać atak?**

Każda usługa udostępniania przez EA jest zarejestrowana pod unikalnym adresem subdomeny, na przykład eaplayinvite.ea.com i posiada pointer DNS (rekord A lub CNAME) do konkretnego hostu chmurowego np. ea-invite-reg.azurewebsites.net, który uruchamia żądaną usługę w tle, w tym przypadku serwer aplikacji webowej.

[link - wideo przedstawiające atak](https://www.youtube.com/watch?v=M1aSni70Sq0&amp;amp;feature=youtu.bee)

Jednak z powodu niepoprawnej konfiguracji na platformie Azure, EA zmieniło rekord CNAME ea-invite-reg.azurewebsites.net w taki sposób, że subdomena eaplayinvite.com już na niego nie wskazywała. To oznaczało, że eaplayinvite.ea.com prowadziło do niedziałającego łącza. Mogliśmy więc wykupić i przejąć rekord CNAME adresu ea-invite-reg.azurewebsites.net, dzięki czemu eaplayinvite.com wskazywało na nasze własne konto chmurowe. Ponieważ uzyskaliśmy kontrolę nad subdomeną, dowolny użytkownik klikający w ten link, mógł nieświadomie zostać przekierowany na naszą stronę.

Następnym krokiem było zbadanie, w jaki sposób EA Games skonfigurowało protokół oAuth i dostarcza użytkownikom mechanizm SSO (Single Sign-on). Mechanizm ten zamienia dane logowania użytkownika (login i hasło) na unikalny token SSO, który jest następnie używany do uwierzytelniania w całej sieci EA bez potrzeby ponownego logowania się do poszczególnych usług.

Po wykryciu kilku problemów w implementacji mechanizmu TRUST przez EA, nasz zespół był w stanie przekierować token SSO na naszą porwaną subdomenę eaplayinvite.ea.com.

Dzięki uzyskaniu tokena, atakujący może zalogować się na konto Origin ofiary i przeglądać wszystkie dane na nim przechowywane, włączając w to możliwość kupowania więcej gier i akcesoriów na koszt użytkownika. Potencjalne szkody mogą być ogromne.

EA Games to druga największa firma związana z grami komputerowymi, obsługująca ponad [90 milionów użytkowników](https://news.ea.com/press-release/company-news/electronic-arts-reports-q4-fy18-and-full-year-fy18-financial-results) i wykazująca dochód około [5 miliardów dolarów](https://www.fool.com/investing/2019/01/10/why-electronic-arts-stock-plunged-25-in-2018.aspx). Może się pochwalić produkcją dobrze znanych serii takich jak FIFA, Maden NFL, NBA Live, UFC, The Sims, Battlefield, Command and Conquer czy Medal of Honor. Wszystkie te gry są dostępne na autorskiej platformie firmy, Origin, która pozwala na zakup oraz granie w gry na PC i urządzeniach mobilnych.

Origin posiada również funkcje społeczne takie jak zarządzanie profilem, zapraszanie innych użytkowników do znajomych, chat, bezpośrednie dołączanie do gier znajomych, a także integracja z platformami społecznościowymi takimi jak Facebook, Xbox Live, PlayStation Network oraz Nintendo Network.