**Krytyczne luki w zabezpieczeniach platformy Friend.tech, doprowadziły do wycieku? Eksperci Check Point Research potwierdzają podatności.**

**Friend.tech, nowa zdecentralizowana platforma społecznościowa (DeSo), która opiera się na handlu „udziałami” umożliwiającymi użytkownikom kontakt z influencerami, oskarżona została jakiś czas temu o wyciek danych przeszło 100 tys. użytkowników. Twórcy platformy natychmiastowo zdementowali plotki, jednak badania przeprowadzone przez ekspertów z Check Point Research wskazują, że Friend.tech posiadał krytyczne luki bezpieczeństwa.**

Friend.tech to coś więcej niż typowa platforma mediów społecznościowych. Jest to jedna z najnowszych platform [web3](https://blog.checkpoint.com/security/from-bitcoin-to-the-metaverse-the-current-evolution-is-a-revolution/), która opiera się na blockchainie i zdecentralizowanych modelach finansowych. Działa jako zdecentralizowany ekosystem, w którym popularność użytkownika wykracza poza zwykłe polubienia i retweety, bowiem przekształca się w tokeny. Można wyobrazić ją sobie jako giełdę osobowości, gdzie wartość zmienia się w odpowiedzi na dynamikę podaży i popytu. Po połączeniu konta użytkownika friend.tech z kontem X (dawniej Twitter), platforma umożliwia użytkownikom handel popularnością poprzez kupno i sprzedaż swoich „udziałów”.

Platforma, uruchomiona w sierpniu 2023 r., pojawiła się na scenie, wzbudzając emocje wśród społeczności web3 i dziennikarzy technologicznych. W stosunkowo krótkim czasie Friend.tech odnotował wyjątkowy wolumen w wysokości 38 884 ETH (w przybliżeniu 64,6 miliona dolarów), który rozdysponowano w ramach 1,5 miliona transakcji. Taki występ nie tylko przykuł uwagę; umocniło to pozycję Friend.tech, plasując ją na drugim miejscu w globalnej aktywności protokołów on-chain.

Chociaż Friend.tech oferuje unikalny sposób czerpania zysków z interakcji społecznych, warto się upewnić, czy jednocześnie zapewnia bezpieczeństwo danych. Sprawdzili to specjaliści ds. cyberbezpieczeństwa z Check Point Research. Wyniki badania nie okazały się pomyślne dla twórców platformy. **Eksperci zidentyfikowali krytyczne luki, których wykorzystanie może umożliwić osobie atakującej dostęp do bazy danych Friend.tech, zapewniającej nieautoryzowaną kontrolę nad różnymi funkcjami, w tym możliwość pobrania całej bazy danych.**

Co więcej, analitycy bezpieczeństwa ustalili, że możliwe jest pobranie wszystkich prywatnych czatów znajdujących się za zaporą. Oznacza to, że rozmowy, które mają być widoczne tylko dla użytkowników, którzy zapłacili, mogą być otwierane i ujawniane bez autoryzacji! Potencjalny atakujący mógłby również zmodyfikować wartości bazy danych, a konkretnie – „punkty” rankingowe (zdobywane poprzez kupno/sprzedaż udziałów użytkowników).

Na początku września firma zespół Check Point Research podzielił się swoimi odkryciami z Friend.tech. Analitycy Check Pointa zalecają wszystkim użytkownikom zachowanie czujności i pamiętanie o właściwych praktykach bezpieczeństwa.