Bitdefender

Converso wycofuje aplikację ze sklepów z powodu ogromnej luki w zabezpieczeniach

19.05.2023

Converso, stosunkowo nowa usługa przesyłania wiadomości zorientowana na prywatność, wycofała swoją aplikację zarówno ze sklepów z aplikacjami Google, jak i Apple w związku z rosnącymi obawami dotyczącymi poważnej luki w zabezpieczeniach. Działania firmy są odpowiedzią na wyniki prywatnego śledztwa przeprowadzonego przez niezależnego blogera.

Brak odpowiednich zabezpieczeń

Crnković, niezależny bloger znany ze swojego wielkiego zainteresowania protokołami szyfrowania i systemami antywirusowymi, odkrył lukę podczas analizy wersji aplikacji Converso na Androida.

Jego analiza ujawniła odniesienia zarówno do algorytmów szyfrowania AES (Advanced Encryption Standard), jak i RSA (Rivest-Shamir-Adleman), mechanizmów, które stanowią podstawę obiecanej przez Converso bezpiecznej komunikacji. Bloger zauważył również wbudowany zestaw do tworzenia oprogramowania (SDK) firmy Seald, uznanego dostawcy szyfrowania i uwierzytelniania za pomocą klucza publicznego.

Niepokojącym aspektem ustaleń Crnkovicia była także niezabezpieczona przez żaden system antywirusowy baza danych hostowana w Google Cloud, z którą komunikowała się aplikacja. Ta baza danych, niepokojąco dostępna dla ogółu społeczeństwa, zawierała szereg poufnych informacji: zaszyfrowaną treść wiadomości, prywatne klucze szyfrujące, metadane wiadomości, a nawet numery telefonów użytkowników.

Szybka reakcja – Converso wycofuje aplikację

Firma Converso podjęła szybkie kroki w celu złagodzenia skutków tego prywatnego śledztwa. Oprócz wycofania swojej aplikacji ze sklepów Google i Apple firma wyczyściła swoją witrynę internetową z wszelkich twierdzeń, że oferuje szyfrowanie typu end-to-end.

„Luka w zabezpieczeniach reguł Firebase została załatana i zapraszamy do jej przetestowania” — odpowiedziała firma Crnkovićowi. – „Inna luka w predefiniowanych kluczach deszyfrujących jest już zaimplementowana po naszej stronie, czekamy tylko na uzyskanie nowych poświadczeń, aby obecni użytkownicy zostali ponownie uwierzytelnieni. Jednak wszystkie istniejące wiadomości wysłane ze starymi kluczami deszyfrującymi są

chronione przez reguły Firebase, więc nadal nie mogą być odczytane przez strony zewnętrzne”.

To odkrycie rodzi pytania o zasadność twierdzeń Converso na temat kompleksowego szyfrowania i solidności jego ogólnych ram bezpieczeństwa.

„Prawidłowo zaimplementowane szyfrowanie typu end-to-end gwarantuje, że nadawca i odbiorca widzą treść wiadomości. Ponadto w tym scenariuszu sam usługodawca nie powinien być w stanie go odszyfrować. Jednak obecność prywatnych kluczy szyfrujących w ujawnionej bazie danych może umożliwić dowolnej osobie mającej dostęp do tych kluczy potencjalne odszyfrowanie zaszyfrowanych wiadomości, naruszając prywatność użytkowników” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/converso-wycofuje-aplikacje-ze-sklepow/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 19.05.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony

użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.