Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

DC.WAC.7351.2.2023

Warszawa, dnia 31.01.2024 r.

Pan
Marcin Wiącek
Rzecznik Praw Obywatelskich

Szanowny Panie Rzeczniku,

w odpowiedzi na wystąpienie z dnia 5 października 2023 r. **dotyczące cyberataków typu *"juice jacking"***, uprzejmie informuję, że w ramach podległego mi Ministerstwa Cyfryzacji zostały podjęte odpowiednie kroki w celu zwiększenia bezpieczeństwa cyfrowego obywateli.

„Juice jacking" jest wektorem ataku wykorzystującym złącze USB, którego obsługa jest zaimplementowana na poziomie systemu operacyjnego telefonu np. Android, iPhone. W zależności od scenariusza, atak może być oparty wyłącznie na socjotechnice, czyli nakłonieniu użytkownika do wykonania konkretnej akcji lub przy wykorzystaniu podatności w systemie operacyjnym umożliwiającej obejście mechanizmów bezpieczeństwa. W przypadku metody opartej na socjotechnice użytkownik nadaje dostęp do odczytu danych urządzenia lub pozwala na instalację dodatkowego oprogramowania, którego zadaniem będzie przejęcie kontroli nad urządzeniem. W przypadku wykorzystania podatności dostęp do urządzenia następuje bez wiedzy i bez interakcji użytkownika.

Projektując aplikację mObywatel uwzględniono zagrożenia związane z nieuprawnionym dostępem do urządzenia oraz możliwością uruchomienia złośliwego oprogramowania na urządzeniu. W tym celu zastosowano następujące , niżej opisane, mechanizmy.

1. Warunkiem uruchomienia aplikacji jest prawidłowe działanie urządzenia oraz systemu operacyjnego, w tym sprawdzenie, czy telefon nie został poddany operacji *„rootowania"*, czyli obejścia podstawowych mechanizmów bezpieczeństwa zapewniających między innymi izolację pomiędzy wątkami procesora, co ogranicza możliwość dostępu do pamięci innych programów. W przypadku, gdy użytkownik poddał *„rootowaniu"* urządzenie, nie jest możliwe zapewnienie odpowiedniego poziomu poufności przetwarzanych danych i aplikacja nie uruchamia się.
2. Wykorzystanie mechanizmów kryptograficznych dostarczanych przez system operacyjny służących do zabezpieczania danych w spoczynku. Wszystkie dane są przechowywane w dedykowanym kontenerze w postaci zaszyfrowanej. Dostęp do danych możliwy jest dopiero po prawidłowym uwierzytelnieniu w aplikacji. Poza zapewnieniem poufności danych osobowych użytkownika, mechanizmy kryptograficzne zapewniają ich integralność dzięki podpisaniu ich pieczęcią ministra. W momencie opuszczania kontenera dane są dodatkowo podpisywane kluczem użytkownika.
3. Wykorzystanie mechanizmów kryptograficznych dostarczanych przez system operacyjny służących do zabezpieczania transmisji danych. Mowa tutaj o mechanizmach zapewniających integralność danych przekazywanych do interesariuszy oraz poufność np. poprzez mechanizm *Certificate Pinning*.

telefon: +48 22 245 59 22
adres email: sekretariat.dc@cyfra.gov.pl
adres strony internetowej: www.gov.pl/cyfryzacja

adres:
00-060 Warszawa
ul. Królewska 27

Bezpieczeństwo cyfrowe jest kluczowe dla naszych obywateli i dlatego podległy mi urząd podejmuje wszelkie możliwe kroki, aby zapewnić ochronę przed takimi atakami. Oprócz bieżących działań mających na celu poprawę bezpieczeństwa naszych systemów, Ministerstwo Cyfryzacji prowadzi również szereg inicjatyw edukacyjnych skierowanych do obywateli. Mają one na celu zwiększenie świadomości na temat zagrożeń cyfrowych i sposobów ich unikania.

W kontekście profilaktyki i przeciwdziałania atakom typu "*juice jacking*", Ministerstwo Cyfryzacji promuje praktyki związane z unikaniem publicznych ładowarek oraz zaleca obywatelom korzystanie z prywatnych źródeł zasilania, power-banków, używanie kabli tylko do ładowania (*only charge*) nieprzesyłających danych cyfrowych oraz systematyczne aktualizowanie systemów operacyjnych i aplikacji.

Ponadto, prowadzone są kampanie informacyjne w mediach społecznościowych i tradycyjnych, aby dotrzeć do jak największej liczby obywateli. Wierzę, że im więcej osób będzie świadomych zagrożeń cyfrowych i sposobów ich unikania, tym bardziej wzrośnie poziom bezpieczeństwa całego społeczeństwa. Materiały edukacyjne Ministerstwa Cyfryzacji są dostępne online i są regularnie aktualizowane, aby odzwierciedlać najnowsze zagrożenia i strategie obronne.

Dalsze informacje na ten temat można znaleźć na stronie internetowej Ministerstwa Cyfryzacji oraz w materiałach edukacyjnych dostępnych dla obywateli. Zachęcam do zapoznania się z nimi w celu zwiększenia świadomości na temat zagrożeń cyfrowych i sposobów ich unikania.

Z wyrazami szacunku

Paweł Olszewski
Sekretarz Stanu
Ministerstwo Cyfryzacji
/dokument podpisany elektronicznie/