Szef CSIRT MON
płk Piotr SOCIK

DOWÓDZTWO KOMPONENTU
WOJSK OBRONY CYBERPRZESTRZENI
K A N C E L A R I A
Nr. 1564/25
2025 -01- 28
VII 05-119 Legionowo VII

MC
RPW/7302/2025 P
Data: 2025-01-31

Sprawa: DKWOC-SBC.OZC.WWC.6424.1.2025
Legionowo, 27 stycznia 2025 r.

Pani Katarzyna ZAJKOWSKA
Dyrektor
Departament Transformacji Cyfrowej
Ministerstwo Cyfryzacji

ul. Królewska 27
00-060 Warszawa

dotyczy: aplikacji mObywatel

Szanowna Pani Dyrektor

W nawiązaniu do pisma w sprawie aplikacji mObywatel (pismo nr DTC.Z-333/2024), uprzejmie informuję, że po przeprowadzonej analizie zagadnienia, stwierdzić należy, że zapisy art. 81a pkt 1 Ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel nakładają na Ministra właściwego do spraw informatyzacji obowiązek udostępnienia kodu źródłowego aplikacji. Jednakże, zdaniem CSIRT MON takie **udostępnienie powinno umożliwiać jedynie wgląd w kod** (bez możliwości pobierania) **oraz zapewnić pełną rozliczalność użytkowników** (np. logowanie z wykorzystaniem profilu zaufanego lub potwierdzenia aplikacją mObywatel), a jego dostępność powinna zostać ograniczona tylko do obywateli RP.

Nadmienić należy, że chociaż kod można uznać za publicznie dostępny (może zostać uzyskany poprzez proces analizy wstecznej - w przypadku systemu android, użyty obfuskator ProGuard jest bardzo minimalistyczny i "zaciemnia" jedynie własne nazwy klas, metod i pól) to przesłane przez Ministerstwo źródła zawierają szereg potencjalnie ciekawych informacji, których nie da się uzyskać poprzez proces analizy wstecznej, a mogą wpłynąć na bezpieczeństwo aplikacji. Są to:

1. Komentarze kodu.
   a) informacje o bibliotekach używanych na serwerze backend;
   b) imiona, nazwiska i nicki programistów aplikacji fronted;

tel.: 261-865-705, 262-762-501
sekretariat.dkwoc@mon.gov.pl
www.wojsko-polskie.pl/woc

ul. gen. T. Buka 1
05-119 Legionowo

c) informacje o używanych narzędziach (nazwy narzędzi lub linki do serwisów).

2. Pliki, które nie pojawiają się w składzie skompilowanej aplikacji.
   a) informacje w plikach, które nie są kodem aplikacji (np. pliki konfiguracyjne używanych narzędzi);
   b) linki do paczek, które są instalowane w środowisku budowania aplikacji.
3. Kod, który jest nieużywany (tzn. dead-code, który potencjalnie mógłby zostać usunięty podczas kompilacji i nie być zawarty w aplikacji dostępnej do pobrania).

Powyższe implikuje konieczność ponownej analizy kodu i usunięcia zbędnych/nadmirowych informacji.

Podsumowując, pomimo, że publikacja kodu niesie pewne ryzyko (np. supply chain attack lub atak na twórców/programistów), to również może przynieść pewne korzyści - np. może zwiększyć zaufanie obywateli do aplikacji oraz utrudnić skompromitowanie mObywatela poprzez dodanie złośliwego kodu (analiza/sprawdzenie kodu przez internautów), w opinii CSIRT MON, **Minister właściwy do spraw informatyzacji może udostępnić kod źródłowy aplikacji mObywatel**, przy zapewnieniu bezpieczeństwa publikowanej informacji (integralność, dostępność, rozliczalność).

Z poważaniem

ppłk Piotr SOCIK

tel.: 261-865-705, 262-762-501
sekretariat.dkwoc@mon.gov.pl
www.wojsko-polskie.pl/woc

ul. gen. T. Buka 1
05-119 Legionowo