

# Raport podsumowujący testy bezpieczeństwa

Produkt: ProteGo Safe

Klient: Ministerstwo Cyfryzacji



KLIENT	Ministerstwo Cyfryzacji
MIEJSCE WYKONANIA TESTÓW	Warszawa
DATA OTWARCIA	04.05.2020
DATA ZAKOŃCZENIA	15.07.2020
OSOBY ODPOWIEDZIALNE	Dominik Maliński Maciej Miszczyk Michał Niwicki Błażej Dusik
WERSJA RAPORTU	1.2



### **SPIS TREŚCI**

1.	POD	SUMOWANIE ZARZĄDCZE	3
2.		ualny status podatności	
3.	Etap	ı – Testy aplikacji mobilnych ProteGo Safe w wersji 3.0	8
	3.1	Podsumowanie techniczne	8
	3.2	Podsumowanie podatności	9
4.	Etap	II – Testy aplikacji mobilnych ProteGo Safe w wersji 4.1, część webowa oraz backend	. 11
	4.1	Podsumowanie techniczne	. 11
	4.2	Podsumowanie podatności	. 12
5.	Etap	ı III – Test aplikacji mobilnych ProteGo Safe w wersji 4.2.1 w modelu PWA Offline	. 14
	5.1	Podsumowanie techniczne	. 14
	5.2	Podsumowanie podatności	. 15
6.	Opis	podatności	. 16
	6.1.	SEQ20200500301	. 16
	6.2.	SEQ20200500302	. 16
	6.3.	SEQ20200500303	. 17
	6.4.	SEQ20200500304	
	6.5.	SEQ20200500305	
	6.6.	SEQ20200500306	
	6.7.	SEQ20200500307	
	6.8.	SEQ20200500308	
	6.9.	SEQ20200500309	
	6.10.	SEQ20200500310	
	6.11.	SEQ20200500311	
	6.12.	SEQ20200500312	
	6.13.	SEQ20200500313	
	6.14.	SEQ20200500314	
	6.15.	SEQ20200600201	
	6.16.	SEQ20200600202	
	6.17.	SEQ20200600203	
	6.18.	SEQ20200600204	
	6.19.	SEQ20200600205	
	6.20.	SEQ20200600206	. 34



#### 1. PODSUMOWANIE ZARZĄDCZE

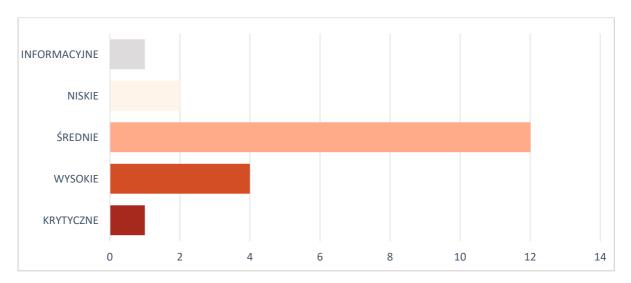
Poniższy dokument stanowi podsumowanie prac zleconych przez Ministerstwo Cyfryzacji firmie SEQRED S.A. w zakresie oceny bezpieczeństwa rozwiązania ProteGo Safe.

Prace przeprowadzone zostały w 3 etapach:

- Etap I Testy bezpieczeństwa aplikacji mobilnych ProteGo Safe dla systemów Android oraz iOS w wersji 3.0
- Etap II Testy bezpieczeństwa aplikacji mobilnych ProteGo Safe dla systemów Android oraz iOS w wersji 4.1, część webowa oraz backend
- Etap III Testy bezpieczeństwa aplikacji mobilnych ProteGo Safe dla systemów Android oraz iOS w wersji 4.2.1 po wprowadzonej zmianie architektury na model PWA Offline

Wszystkie zidentyfikowane podczas wyżej opisanego cyklu testów podatności zostały naprawione lub uniemożliwiono ich wykorzystanie w wersji 4.2.1. W ostatniej testowanej wersji aplikacji 4.2.1 nie zostały zidentyfikowane żadne dodatkowe podatności.

Wyniki prac wyszczególnione dla każdego z etapów zostały opisane w rozdziałach 3, 4 i 5. Łącznie we wszystkich etapach testów zidentyfikowano 20 podatności. Poniżej podsumowano rozkład liczby podatności w ujęciu ich krytyczności.



Wykres 1. Zestawienie zidentyfikowanych podatności



#### Zakres testów

Celem przeprowadzonych testów była identyfikacja podatności w rozwiązaniu ProteGo Safe.

#### Zakres prac dla aplikacji mobilnych obejmował:

- Przeprowadzenie analizy statycznej kodu źródłowego aplikacji dla systemów Android oraz iOS,
  łącznie z analizą biblioteki służącej do lokalizacji urządzenia mobilnego. Narzędzia wykorzystane
  dla tego kroku to dla aplikacji Android (napisanej z wykorzystaniem języka Kotlin) ktlint oraz
  detekt, dla aplikacji iOS (napisanej z wykorzystaniem języka Swift) SwiftLint oraz Clang Static
  Analyzer,
- Manualna weryfikacja wytypowanych błędów oraz warningów będących wynikiem analizy statycznej (potwierdzenie, odrzucenie),
- Weryfikacja wykorzystanych mechanizmów komunikacji IPC (Inter-Process-Communication)
  pomiędzy komponentami aplikacji lub/i komponentami firm trzecich pod kątem
  nieuprawnionego dostępu skutkującego pozyskaniem wrażliwych informacji lub wstrzyknięcia
  nieprawidłowych danych,
- Weryfikacja poprawności wykorzystania systemowego API,
- Przeprowadzenie weryfikacji zgodnie z metodyką CyberSecurity Bill of Materials określenie istniejących i znanych podatności dla bibliotek zewnętrznych wykorzystywanych w aplikacji,
- Weryfikacja metod ekspozycji i utrzymywania wrażliwych danych weryfikacja ich lokalizacji
  oraz ew. logowania danych do logów systemu operacyjnego, ze szczególnym uwzględnieniem
  danych (rekordów) z biblioteki służącej do lokalizacji, określających historię kontaktów z innymi
  użytkownikami aplikacji ProteGO Safe,
- Weryfikacja wykorzystanych rodzajów szyfrowania i poprawności szyfrowania dla danych, ze szczególnym uwzględnieniem rekordów biblioteki służącej do lokalizacji – weryfikacja zastosowanych algorytmów szyfrowania i hashowania wraz z przeprowadzeniem próby przełamania zabezpieczeń,
- Weryfikacja wykorzystanych rodzajów szyfrowania i poprawności szyfrowania dla kanałów komunikacji, w szczególności pomiędzy aplikacjami mobilnymi a aplikacją webową oraz API – weryfikacja zastosowanych algorytmów szyfrowania i hashowania, konfiguracji mechanizmów szyfrowania oraz wymiany kluczy,
- Weryfikacja występowania wrażliwych danych w kodzie aplikacji pod kątem pozostawienia w kodzie lub plikach aplikacji danych takich jak hasła i klucze prywatne,
- Weryfikacja występowania wrażliwych danych w plikach aplikacji, pamięci nieulotnej urządzenia mobilnego, logach, pamięci podręcznej (cache), niezabezpieczonej bazie SQLite,
- Weryfikacja czy ww. wrażliwe dane z biblioteki służącej do lokalizacji są czyszczone z wymienionych lokalizacji po upływie określonego czasu,
- Weryfikacja poprawności zaimplementowanych mechanizmów typu Certificate Pinning, podejmując próbę ataku MitM (Man in the Middle) ze szczególnym uwzględnieniem komponentu WebView (wyświetlającego treści m.in z https://safesafe.app/),



- Weryfikacja możliwości złośliwego wykorzystania natywnego interfejsu JavaScript wykorzystanego w aplikacji zarejestrowanego pod nazwą "NativeBridge" (zdefiniowanego w NativeBridgeInterface.kt dla systemu Android oraz JSBridge.swift dla systemu iOS),
- Dynamiczna analiza komunikacji Bluetooth pomiędzy dwoma urządzeniami wykorzystującymi
  aplikację ProteGO Safe ze szczególnym uwzględnieniem bezpieczeństwa wymiany komunikatów
  z wykorzystaniem biblioteki służącej do lokalizacji. Zbadanie odporności biblioteki na ataki
  z OWASP TOP 10 ze szczególnym uwzględnieniem ataków charakterystycznych dla
  wykorzystywanej technologii tj. injection, replay i relay attack,
- Na podstawie potencjalnie odnalezionych błędów przygotowanie scenariuszy ataku uwzględniającego przejęcie i zdeszyfrowanie rekordów biblioteki służącej do lokalizacji.

#### Zakres prac dla części webowej oraz API obejmował:

- Analiza dostarczonej dokumentacji pod kątem identyfikacji stacku technologicznego, elementów architektury aplikacji oraz API,
- Ocena przyjętej koncepcji i architektury rozwiązania ProteGO Safe pod kątem zapewnienia anonimowości oraz poufności użytkowników,
- Enumeracja potencjalnie exploitowalnych adresów (URL'i, endpointów usług REST/SOAP),
   niezabezpieczonych katalogów lub innych wrażliwych kontekstów, ze szczególnym
   uwzględnieniem paneli administracyjnych, narzędzi deweloperskich lub administracyjnych,
   statystyki serwera oraz katalogów zawierających wrażliwe dane, (np. pliki konfiguracyjne),
- Weryfikacja stacku technologicznego wdrożonego produktu pod kątem znanych podatności –
  przeszukanie baz z podatnościami (MITRE, CVE, exploit-db) posługując się informacjami z
  zebranych banerów, przekazanymi przez klienta, uzyskanymi w wyniku rekonesansu, kodu
  źródłowego lub skanów wykonanych na środowisku testowym,
- Identyfikacja możliwych punktów wprowadzania danych i interakcji z użytkownikiem, identyfikacja różnic w walidacji między komponentami frontendowymi, a funkcjonalnością logiki biznesowej komponentów backendowych poprzez próby wykonania bezpośrednich zapytań do endpointów z pominięciem weryfikacji na stronach źródłowych.
- Przeprowadzenie testów penetracyjnych w celu identyfikacji podatności, ze szczególnym uwzględnieniem podatności OWASP TOP 10, wraz z użyciem automatycznych skanerów posiadających bazę złośliwych danych wejściowych w postaci: SQL, JavaScript, HTML, XML, CSV.
   Przeprowadzenie testów aplikacji z perspektywy użytkownika – wykonanie typowych akcji użytkownika na rożnych przeglądarkach w trybie debug,
- Próby zachwiania prawidłowego przebiegu procesu biznesowego poprzez manipulację przesyłanymi danymi,
- Testy walidacji danych wejściowych.



#### 2. Aktualny status podatności

Podatności zidentyfikowane w Etapach I, II i III zostały przekazane do analizy zespołowi odpowiedzialnemu za rozwój rozwiązania ProteGO Safe, a następnie po przeprowadzeniu działań naprawczych poddane retestom. Status usunięcia odnalezionych podatności w odniesieniu do ostatnich testowanych wersji aplikacji t.j. 4.2.1, został przedstawiony poniżej.

Wszystkie zidentyfikowane podatności zostały naprawione lub uniemożliwiono ich wykorzystanie.

ID	PRIORYTET	PODATNOŚĆ	OPIS	STATUS v4.2.1
SEQ20200500301	ŚREDNI	Logowanie wrażliwych danych	[Android] Wyciek tokenów Firebase w logach systemowych	Naprawione
SEQ20200500302	NISKI	Brak mechanizmu root detection	[Android] Aplikacja nie posiada wbudowanego mechanizmu root detection	Naprawione
SEQ20200500303	NISKI	Brak mechanizmu jailbreak detection	[iOS] Aplikacja nie posiada wbudowanego mechanizmu jailbreak detection	Naprawione
SEQ20200500304	ŚREDNI	Nieszyfrowane dane wrażliwe	[Android] Dane wrażliwe - plik zawierający listę tempID nie jest szyfrowany w pamięci nieulotnej	Nie dotyczy
SEQ20200500305	ŚREDNI	Nieszyfrowane dane wrażliwe	[Android] Dane wrażliwe – baza danych zawierająca listę odczytanych tempID nie jest szyfrowana w pamięci nieulotnej	Nie dotyczy
SEQ20200500306	ŚREDNI	Nieszyfrowane dane wrażliwe – dane medyczne uzupełnione w trakcie ankiety nie są szyfrowane w pamięci nieulotnej		Nie dotyczy
SEQ20200500307	ŚREDNI	Nieszyfrowane dane wrażliwe	[iOS] Dane wrażliwe - plik zawierający listę tempID nie jest szyfrowany w pamięci nieulotnej	Nie dotyczy
SEQ20200500308	ŚREDNI	Nieszyfrowane dane wrażliwe	[iOS] Dane wrażliwe – baza danych zawierająca listę odczytanych tempID nie jest szyfrowana w pamięci nieulotnej	Nie dotyczy
SEQ20200500309	ŚREDNI	Niewystarczająca walidacja certyfikatów	[Android] Brak zaimplementowanego mechanizmu certificate-pinning	Naprawione



SEQ20200500310	ŚREDNI	Niewystarczająca walidacja certyfikatów	[iOS] Brak zaimplementowanego mechanizmu certificate-pinning	Naprawione	
SEQ20200500311	ŚREDNI	Włączony backup	[Android / iOS] Aplikacje pozwalają na wykonywanie backupów		
SEQ20200500312	ŚREDNI	[Android] Ograniczenia dotyczące czasu przechowywania i usuwania tymczasowych identyfikatorów mogą zostać ominięte poprzez modyfikację czasu systemowego		Nie dotyczy	
SEQ20200500313	INFO	Błąd logiczny	[iOS] Tymczasowe identyfikatory napotkanych urządzeń nie są usuwane z bazy danych	Nie dotyczy	
SEQ20200500314	ŚREDNI	Podatności kryptograficzne protokołów	[Android / iOS] Możliwość przeprowadzenia ataków typu relay attack	Nie dotyczy	
SEQ20200600201	KRYTYCZNY	Enumeracja wrażliwych danych	[Backend] Możliwość enumeracji poprawnych kodów PIN dla endpointa /getAccessToken	Naprawione	
SEQ20200600202	WYSOKI	Brak mechanizmu rate-limiting	[Backend] Brak limitu żądań dla serwisu /getAccessToken	Naprawione	
SEO 20200600 203 WVSOK		[Backend] Brak limitu żądań dla serwisu /generateCode	Naprawione		
SEQ20200600204	Ominięcie wbudowanych		Brak możliwości wykorzystania ze względu na wprowadzone kroki naprawcze dla powiązanych podatności		
SEQ20200600205	WYSOKI	Ominięcie wbudowanych mechanizmów zabezpieczających	[Android] Możliwość obejścia mechanizmu ograniczenia ilości prób wpisania kodu PIN	Brak możliwości wykorzystania ze względu na wprowadzone kroki naprawcze dla powiązanych podatności	
SEQ20200600206	ŚREDNI	Brak nagłówków http	[Backend] Brak nagłówków http odpowiedzialnych za bezpieczeństwo (Strict- Transport-Security, X-Frame- Options, X-XSS-Protection), brak mechanizmu Content Security Policy	Naprawione	



#### 3. Etap I – Testy aplikacji mobilnych ProteGo Safe w wersji 3.0

#### 3.1 Podsumowanie techniczne

Lokalizacja testów	Warszawa
Data rozpoczęcia	04.05.2020
Data zakończenia	15.05.2020
Nazwa aplikacji, Android	ProteGO Safe
Wersja aplikacji, Android	3.0.3
Nazwa pakietu, Android	pl.gov.mc.protegosafe
Sumy kontrolne, Android	MD5:c70fa1e8edbe06e9fa1d29ddd540518c SHA1:fec8c5859c1e24943aeadeafc9d0c1482ad90254 SHA256:03e116b831b184842ea96bb17f7880439addf5cb724da54c735b73 0f34eb44dc
Nazwa aplikacji, iOS	ProteGO Safe
Wersja aplikacji, iOS	3.0.2
Identyfikator, iOS	pl.gov.mc.protegosafe
Sumy kontrolne, iOS	MD5:9074acc39c6ab0c063caaec769ecc848 SHA1:188fb3dd1d7bfebc73ab5dda4292df7c4da7e2e2 SHA256:2edd10c6da64c3d9b638f19c91d3d7337259f36b3fc50f4016aca5df d6e65e90

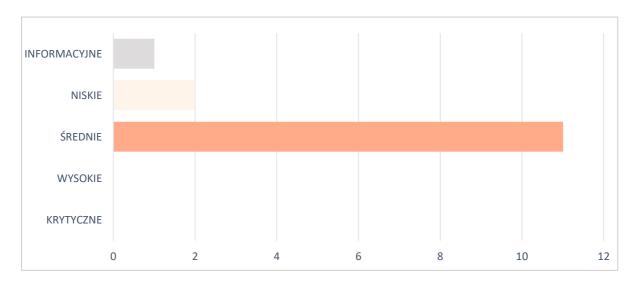
Aplikacje mobilne ProteGo Safe zostały poddane testom penetracyjnym. Prace zostały zrealizowane zgodnie z metodyką opisaną w OWASP Mobile Application Security Verification Standard (MASVS) oraz zaleceniami OWASP Mobile Security Testing Guide (MSTG).

Testowane aplikacje zostały pobrane z oficjalnych kanałów, Google Play oraz AppStore. Testy przeprowadzone zostały w formule white-box, z dostępem do publicznego repozytorium projektu ProteGo Safe znajdującego się pod adresem https://github.com/ProteGO-Safe.



#### 3.2 Podsumowanie podatności

W trakcie realizacji pierwszego etapu testów ujawniono istnienie 14 podatności, których zestawienie ilościowe oraz ocena krytyczności zostały zebrane w tabelach poniżej.



ID	PRIORYTET	PODATNOŚĆ	OPIS	
SEQ20200500301	ŚREDNI	Logowanie wrażliwych danych	[Android] Wyciek tokenów Firebase w logach systemowych	
SEQ20200500302	NISKI	Brak mechanizmu root detection	[Android] Aplikacja nie posiada wbudowanego mechanizmu root detection	
SEQ20200500303	NISKI	Brak mechanizmu jailbreak detection	[1.2.0] . Ib because	
SEQ20200500304	ŚREDNI	Nieszyfrowane dane wrażliwe	[Android] Dane wrażliwe - plik zawierający listę tempID nie jest szyfrowany w pamięci nieulotnej	
SEQ20200500305	ŚREDNI	Nieszyfrowane dane wrażliwe	[Android] Dane wrażliwe – baza danych zawierająca listę odczytanych tempID nie jest szyfrowana w pamięci nieulotnej	
SEQ20200500306	ŚREDNI	Nieszyfrowane dane wrażliwe	[Android] Dane wrażliwe – dane medyczne uzupełnione w trakcie ankiety nie są szyfrowane w pamięci nieulotnej	
SEQ20200500307	ŚREDNI	Nieszyfrowane dane wrażliwe	[iOS] Dane wrażliwe - plik zawierający listę tempID nie jest szyfrowany w pamięci nieulotnej	
SEQ20200500308	ŚREDNI	Nieszyfrowane dane wrażliwe	[iOS] Dane wrażliwe – baza danych zawierająca listę odczytanych tempID nie jest szyfrowana w pamięci nieulotnej	



ID	PRIORYTET	PODATNOŚĆ	OPIS
SEQ20200500309	ŚREDNI	Niewystarczająca walidacja certyfikatów	[Android] Brak zaimplementowanego mechanizmu certificate-pinning
SEQ20200500310	ŚREDNI	Niewystarczająca walidacja certyfikatów	[iOS] Brak zaimplementowanego mechanizmu certificate-pinning
SEQ20200500311	ŚREDNI	Włączony backup	[Android / iOS] Aplikacje pozwalają na wykonywanie backupów
SEQ20200500312	ŚREDNI	Błąd logiczny	[Android] Ograniczenia dotyczące czasu przechowywania i usuwania tymczasowych identyfikatorów mogą zostać ominięte poprzez modyfikację czasu systemowego
SEQ20200500313	INFO	Błąd logiczny	[iOS] Tymczasowe identyfikatory napotkanych urządzeń nie są usuwane z bazy danych
SEQ20200500314	ŚREDNI	Podatności kryptograficzne protokołów	[Android / iOS] Możliwość przeprowadzenia ataków typu relay attack



# 4. Etap II – Testy aplikacji mobilnych ProteGo Safe w wersji 4.1, część webowa oraz backend

#### 4.1 Podsumowanie techniczne

Lokalizacja testów	Warszawa
Data rozpoczęcia	03.06.2020
Data zakończenia	18.06.2020
Nazwa aplikacji, Android	ProteGO Safe
Wersja aplikacji, Android	4.1.0
Nazwa pakietu, Android	pl.gov.mc.protegosafe
Sumy kontrolne, Android	MD5:5332df166082ccd5e35c6954d2ab6ade SHA1:8f8ed4c0f0e5dc7397b7aa5d159dcb355fa1bc5f
Nazwa aplikacji, iOS	ProteGO Safe
Wersja aplikacji, iOS	4.1.1
Identyfikator, iOS	pl.gov.mc.protegosafe
Sumy kontrolne, iOS	MD5:da7a3451b99eb7bd13ff1aa27794d17a SHA1:f0e5e95fcca5343a5d355842855d888cc4083ae6

#### Testom zostały poddane:

- aplikacje mobilne w wersjach 4.1,
- część webowa, exp.safesafe.app, exp.safesafe.app//index.txt,
- część API, t.j. endpointy /generateCode, /getAccessToken, /uploadDiagnosisKeys

Prace zostały zrealizowane zgodnie z metodykami opisanymi w OWASP Mobile Application Security Verification Standard (MASVS), OWASP Mobile Security Testing Guide (MSTG) oraz OWASP Testing Guide ze szczególnym nastawieniem na zidentyfikowanie podatności opisanych w OWASP Top 10.

W toku uzgodnień potwierdzono wyłączenie z zakresu testów komponentu Centrum Kontaktów.

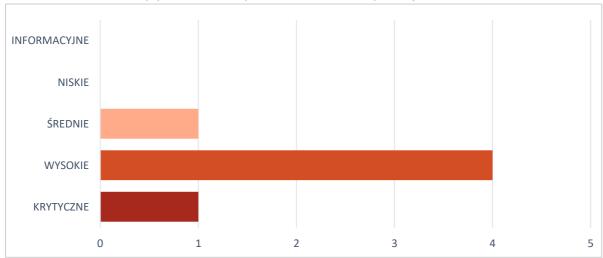
Dostęp do aplikacji mobilnych został zapewniony poprzez dodanie kont audytorów do programów wczesnego dostępu na platformach Google Play oraz AppStore. Dostęp do części webowej oraz backend został zapewniony poprzez udostępnienie środowiska testowego. Testy przeprowadzane były w formule white-box, z dostępem do publicznego repozytorium projektu ProteGo Safe znajdującego się pod adresem <a href="https://github.com/ProteGO-Safe">https://github.com/ProteGO-Safe</a>. W testowanych wersjach aplikacji mobilnych biblioteka OpenTrace została zastąpiona poprzez wykorzystanie API Exposure Notification



(<a href="https://www.google.com/covid19/exposurenotifications/">https://www.google.com/covid19/exposurenotifications/</a>, <a href="https://developer.apple.com/documentation/exposurenotification">https://developer.apple.com/documentation/exposurenotification</a>).

#### 4.2 Podsumowanie podatności

W trakcie realizacji drugiego etapu testów ujawniono istnienie 6 podatności, których zestawienie ilościowe oraz ocena krytyczności zostały zebrane w tabelach poniżej.



ID	PRIORYTET	PODATNOŚĆ	OPIS	
SEQ20200600201	KRYTYCZNY	Enumeracja wrażliwych danych	[Backend] Możliwość enumeracji poprawnych kodów PIN dla endpointa /getAccessToken	
SEQ20200600202	WYSOKI	Brak mechanizmu rate-limiting	[Backend] Brak limitu żądań dla serwisu /getAccessToken	
SEQ20200600203	WYSOKI	Brak mechanizmu rate-limiting	[Backend] Brak limitu żądań dla serwisu /generateCode	
SEQ20200600204	WYSOKI	Ominięcie wbudowanych mechanizmów zabezpieczających	[iOS] Możliwość obejścia mechanizmu ograniczenia ilości prób wpisania kodu PIN	
SEQ20200600205	WYSOKI	Ominięcie wbudowanych mechanizmów zabezpieczających	[Android] Możliwość obejścia mechanizmu ograniczenia ilości prób wpisania kodu PIN	



ID	PRIORYTET	PODATNOŚĆ	OPIS
SEQ20200600206	ŚREDNI	Brak nagłówków http	[Backend] Brak nagłówków http odpowiedzialnych za bezpieczeństwo (Strict-Transport-Security, X-Frame- Options, X-XSS-Protection), brak mechanizmu Content Security Policy



## 5. Etap III – Test aplikacji mobilnych ProteGo Safe w wersji 4.2.1 w modelu PWA Offline

#### 5.1 Podsumowanie techniczne

Lokalizacja testów	Warszawa
Data rozpoczęcia	02.07.2020
Data zakończenia	15.07.2020
Nazwa aplikacji, Android	ProteGO Safe
Wersja aplikacji, Android	4.2.1
Nazwa pakietu, Android	pl.gov.mc.protegosafe
Sumy kontrolne, Android	MD5: 860239022a636f4c0978a3da57677be7
	SHA1: 066cef55f633b0b788beca83c2dd4bd15539e761
Nazwa aplikacji, iOS	ProteGO Safe
Wersja aplikacji, iOS	4.2.1
Identyfikator, iOS	pl.gov.mc.protegosafe
Sumy kontrolne, iOS	MD5: ad06b39d2c4f5f0431a68b50eaf6926e
	SHA1: d09c7eaeeddb4328fa2a837f3ef57be292798731

Aplikacje mobilne ProteGo Safe zostały poddane testom penetracyjnym. Prace zostały zrealizowane zgodnie z metodyką opisaną w OWASP Mobile Application Security Verification Standard (MASVS) oraz zaleceniami OWASP Mobile Security Testing Guide (MSTG).

Dostęp do aplikacji mobilnych został zapewniony poprzez dodanie kont audytorów do programów wczesnego dostępu na platformach Google Play oraz AppStore. Testy powiązane ze zmianą architektury na PWA Offline obejmowały:

- określenie lokalizacji kodu html oraz javascript po zainstalowaniu aplikacji ProteGo Safe na urządzeniu mobilnym
- weryfikację, czy w.w. kod może zostać modyfikowany poprzez aplikacje firm trzecich zainstalowane na urządzeniu mobilnym
- poddanie aplikacji analizie dynamicznej celem określenia ilości requestów sieciowych realizowanych poprzez aplikacje
- weryfikację czy dodatkowy kod html, javascript lub inne zasoby są ładowane z lokalizacji sieciowych
- określenie ilości zewnętrznych serwisów (stron internetowych), do których może zostać zrealizowane przekierowanie w module WebView



#### 5.2 Podsumowanie podatności

W testowanych wersjach 4.2.1 aplikacji dla systemów Android oraz iOS nie wykryto podatności, które zmniejszałyby poziom bezpieczeństwa aplikacji ze względu na wykorzystaną architekturę PWA Offline. Aplikacje utrzymują kod html/javascript w lokalizacjach, które są prywatne dla aplikacji, wykorzystując niezmodyfikowane oprogramowanie urządzenia mobilnego nie ma możliwości modyfikacji kodu poprzez aplikacje firm trzecich. Aplikacje nie pobierają dodatkowych treści z sieci internet, ograniczają komunikację sieciową do minimum podyktowanego wbudowanymi funkcjonalnościami aplikacji. Linki do zewnętrznych domen, które są wbudowane w aplikacje i umożliwiają użytkownikom przeniesienie się na zewnętrzne serwisy, nie są uruchamiane w module WebView, a we wbudowanej w system operacyjny przeglądarce. Czyni to interfejs Javascript Interface wbudowany w aplikacje niedostępny dla zewnętrznych serwisów/stron internetowych.



#### 6. Opis podatności

#### 6.1. SEQ20200500301

PODATNOŚĆ	[Android] Wyciek tokenów Firebase w logach systemowych	PRIORYTET	ŚREDNI		
CVSS VECTOR	AV:N/AC:/PR:L/UI:N/S:U/C:H/I:N/A:N	CVSS:3.0 base score	6.4		
OPIS	Aplikacja ProtegoSafe loguje pełną treść tokenu FCM (registrationToken) i tokenów sesyjnych (refreshedToken). Tokeny te identyfikują konkretną instalację aplikacji na urządzeniu. W przypadku ich wycieku, możliwe jest podsłuchanie przez atakującego wiadomości wysyłanych z Firebase na dane urządzenie (powiadomień push).				
ZALECENIA	Pozbyć się nadmiarowego logowania. Upewnić się, że sekrety i inne dane wrażliwe nie trafiają do logów systemowych.				
SZCZEGÓŁY TECHNICZNE  Fragment logu systemowego zawierający tokeny registrationToken refreshedToken					
		LYR8I8SIyQSnDLWbjwKTRnoqfsE 8DSuVFM1pWzNzwHa2ms4YqLYR83			

#### 6.2. SEQ20200500302

PODATNOŚĆ	[Android] Aplikacja nie posiada wbudowanego mechanizmu root detection	PRIORYTET	NISKI
CVSS VECTOR	AV:P/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	CVSS:3.0 base score	2.4
OPIS	Aplikacja poprawnie uruchamia się i działa na z Użytkownicy posiadający zrootowane urządzer kradzież wrażliwych danych opisanych w SEQ20 oraz SEQ20200500306.	nia są bezpośre	dnio podatni na
ZALECENIA	Wprowadzić mechanizm root-detection.		
SZCZEGÓŁY TECHNICZNE	N/D		



#### 6.3. SEQ20200500303

PODATNOŚĆ	[iOS] Aplikacja nie posiada wbudowanego mechanizmu jailbreak detection	PRIORYTET	NISKI
CVSS VECTOR	AV:P/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	CVSS:3.0 base score	2.4
OPIS	Aplikacja poprawnie uruchamia się i działa na ju Użytkownicy posiadający takie urządzenia są bo kradzież wrażliwych danych opisanych w SEQ20 oraz SEQ20200500308.	ezpośrednio po	odatni na
ZALECENIA	Wprowadzić mechanizm jailbreak-detection.		
SZCZEGÓŁY TECHNICZNE	N/D		



#### 6.4. SEQ20200500304

PODATNOŚĆ	[Android] Dane wrażliwe - plik zawierający listę tempID, nie jest szyfrowany w pamięci nieulotnej	PRIORYTET	ŚREDNI
CVSS VECTOR	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	CVSS:3.0 base score	6.5
OPIS	Tymczasowe identyfikatory utrzymywane są w w pliku /data/data/pl.gov.mc.protegosafe/files uzyska dostęp do systemu plików na urządzeni identyfikatory, które użytkownik rozgłasza I bę czasie.	s/tempIDs. Ata u może pozysk	kujący, który ać
ZALECENIA	Zalecamy wprowadzenie mechanizmu root-de problem dostępu do wrażliwych danych na zro Zalecamy przechowywać tymczasowe identyfik	otowanych urz	ządzeniach.
SZCZEGÓŁY TECHNICZNE	/data/data/pl.gov.mc.protegosafe/files # cat tempIDs  [{"expiryTime":1589114571,"tempID":"btd3HYF7B3V4s8ljwtt4 URtZTbYLLtzK5xdZBoAvfc48xdlWnQ==","startTime":15891136 ":"upRs+G2Jbj1Yi+/A7wfWxmSGVCMXSc76iz1DBM+O3usmhs 2YQ==","sta rtTime":1589114571},{"expiryTime":1589116371,"tempID":"5 prm6csNWX38f+lKksW9tj78zAJoourwAV8tu75WgKu+NFtA==' :1589117271,"tempID":"lr2fe6tu9Mp94KBC3c7gOPjbEvFiRYRI DolQ6DtJf 9J+J1vShM0Q==","startTime":1589116371},{"expiryTime":158 ievE7zbIGQQDQXc9pFSARmpBH0W5WOzOZFu6rPbORbwKSM me":1589117271},{"expiryTime":1589119071,"tempID":"su5P Doujyx8lVrqe2m+ 3f2ifjxmjeH7eCi4GmM1YbfbD2AVcw==","startTime":1589118 D":"AJUSsi2cYtgnxXR3CiLu1bQyCDkrXSHh+kdEE1P/L7QMrmU hsw==","startTime":1589119071},{"expiryTime":1589120871, a2jBITar6 p/hoywnY237DEye55d1PR3f/vl0GGEX46oE3NEs91JJT13EiQ== ":1589121771,"tempID":"6JmFKhG46iAnXJ4a/L/90Vnl9aiwVq 3OYoXzI54t/m7XonxlQ==","startTime":1589120871},{"expiryTix Lgfq hMBl2cMTT95GBO7gVVeLQzTTYCcgp8SvA/Ca+uGVAZHssfQm 589121771},{"expiryTime":1589123571,"tempID":"6gdiPwcxVqLjE6lZCFgw5FwTAdq6/rKbjOFe1hj1ESvbW9aQ==","startTime 71,"temp ID":"MnqyH8m5ateY/QX7h6ERrbAq9BTsVSfEpVXDzdX8hxpCu CitQ==","startTime":1589123571},{"expiryTime":1589125371, OmRuOqLlrqk15Kwl4MlTcM5bhKFa/Sl7ZPvCUX+3JF7USJZxBCl 1},{"expiryTime":1589126271,"tempID":"phl5U2t9gnDFzU2EA0CLtMnVnoITtySavijqaAVzdzyfmZ1EA=="	571},{"expiryTime":1 oBqG2kdfo1vwZP+I- oBqG2kdfo1vwZP+I- c48bVgZtaMztZ+XB ',"startTime":15891 .6Wnzwyewg29SRA B9118171,"tempID": lxzRfQ5O1w4rTnyRI- cQhIYQk86DdIHQ; l171},{"expiryTime": WOZFpPn44Ihqb+OI "tempID":"dW6Ipg2 ","startTime":15891 /6D2SwCgtIml1aP+I Time":1589122671," kMBR9kGxIP92j75q 'XDtFqeIvEFG+VpZV '":1589122671},{"ex hSpsPvCaZeJQfARxS ,"tempID":"Op7Nh7 bpdWoPzYw==","sta	D7drlROtXD3fKof9Jb 15471},("expiryTime" UHtGCub9TH8rPDzd "V3e70V5kXyyTmMS HVVO6Q==","startTi 2UVBqjjKoAKVDdf4X 1589119971,"templ mRUTKsDAd5tZpTgl EulLcCEZQg2SLmCces 19971},{"expiryTime PiVhCk9JZBQFzV1yW templD":"NCl2zuvgt illw==","startTime":1 yE8jRnfyNJ+kXb4jSV piryTime":15891244 fmzj1nHS+RvqDNNk+ 1xAL9A3rLHARYpjbX artTime":158912447



#### 6.5. SEQ20200500305

PODATNOŚĆ	zaw	ierająca list	ę odc	liwe – baza danych zytanych tempID, nie imięci nieulotnej	PRIOR	YTET Ś	REDNI	
CVSS VECTOR	AV:N	N/AC:L/PR:l	_/UI:N	/S:U/C:H/I:N/A:N	CVSS:3 base s	6	.5	
OPIS	są w /dat któr iden	nieszyfrow a/data/pl.g y uzyska do tyfikatory u	vanej l ov.mo stęp o uzysku	katory pobrane z napotkan bazie danych c.protegosafe/databases/re do systemu plików na urząc ijąc informacje dotyczące h eniami i powiązanymi iden	ecord_ dzeniu istorii	database może poz kontaktó	. Atakuj zyskać	ący,
ZALECENIA	prob	lem dostęp	ou do	enie mechanizmu root-dete wrażliwych danych na zroo nie szyfrowania bazy danyc	towan		•	า.
SZCZEGÓŁY				cord_database znajduje się	•	•	rowana	ı
SZCZEGÓŁY TECHNICZNE	/dat Tabl prot	a/data/pl.g ica record_ okołu, tem	ov.mo table pID, ta	cord_database znajduje się c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_	aza nie ące cza zeń, w	e jest szyf asu rozpoz rskaźniki r	znania, ssi oraz	wersji
	/dat Tabl prot txPo	a/data/pl.g ica record_ okołu, tem	ov.mo table pID, ta	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd	aza nie ące cza zeń, w	e jest szyf asu rozpoz rskaźniki r	znania, ssi oraz	wersji
	/dat Tabl prot txPo	a/data/pl.g ica record_ okołu, tem wer. Przykł	table pID, ta	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_	aza nie ące cza zeń, w _table	e jest szyf asu rozpoz rskaźniki r widoczna	znania, rssi oraz jest po	wersji niżej:
	/dat Tabl prot txPo	a/data/pl.g ica record_ okołu, tem wer. Przykł	table pID, ta	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_	aza nie ące cza zeń, w _table	e jest szyf asu rozpo: zskaźniki r widoczna	znania, ssi oraz jest po	wersji niżej:
	/dat Tabl prot txPo	a/data/pl.g ica record_ okołu, tem wer. Przykł record_table id timestamp or Filter 1588649544594	table pID, ta	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_	aza nie ące cza zeń, w _table	e jest szyf asu rozpoz rskaźniki r widoczna	znania, essi oraz jest po modelc Filter	wersji niżej:
	/dat Table prot txPo	a/data/pl.g ica record_ okołu, tem wer. Przykł  record_table id timestamp or   filter   1588649544594   1588649685554   1588649832474	table pID, ta	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_  msg  Filter xuN9eFSSrrcFlgYgK+zcDVpQmdMYIU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFlgYgK+zcDVpQmdMYIU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFlgYgK+zcDVpQmdMYIU872F9jSfbvOFYyKWrdL	aza nie ące cza zeń, w _table	e jest szyf asu rozpoz rskaźniki r widoczna modelp Filter Redmi Note 8 Pro Redmi Note 8 Pro Redmi Note 8 Pro	znania, essi oraz jest po modelc Filter sm-G920F sm-G920F	miżej:  rssi Filter -83 -84 -80
	/dat Tabl prot txPo	a/data/pl.g ica record_ okołu, tem wer. Przykł id timestamp or Filter 1588649685554 1588649685554 1588649832474	ov.mo table pID, ta adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_  msg  Filter xuN9eFSSrrcFigYgK+zcDVpQmdMYiU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFigYgK+zcDVpQmdMYiU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFigYgK+zcDVpQmdMYiU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFigYgK+zcDVpQmdMYiU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFigYgK+zcDVpQmdMYiU872F9jSfbvOFYyKWrdL	aza niegące czazeń, w table	e jest szyf asu rozpoz rskaźniki r widoczna modelP Filter Redni Note 8 Pro Redni Note 8 Pro Redni Note 8 Pro Redni Note 8 Pro	znania, rssi oraz jest po modelc Filter SM-G920F SM-G920F SM-G920F SM-G920F	wersji niżej: rssi Filter -83 -84 -80 -83
	/dat Table prot txPo	a/data/pl.g ica record_ okołu, tem wer. Przykł id timestamp or Filter 1588649685554 1588649685554 1588649832474	ov.mo table pID, ta adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_  msg  Filter xuN9eFSSrrcFlgYgK+zcDVpQmdMYIU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFlgYgK+zcDVpQmdMYIU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFlgYgK+zcDVpQmdMYIU872F9jSfbvOFYyKWrdL	aza niegące cza zeń, w table	e jest szyf asu rozpoz rskaźniki r widoczna modelp Filter Redmi Note 8 Pro Redmi Note 8 Pro Redmi Note 8 Pro	znania, essi oraz jest po modelc Filter sm-G920F sm-G920F	wersji niżej: rssi Filter -83 -84
	/dat Tabl prot txPo  Table    Filth   1   125   2   136   3   131   4   132   5   135	a/data/pl.g ica record_ okołu, tem wer. Przykł record_table id timestamp ir   Filter   15886495354594 1588649832474 1588649923120 1588650168142	ov.mo table pID, ta adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_  msg  Filter xuN9eFSsrrcFigYgK+zcDVpQmdMYiU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFigYgK+zcDVpQmdMYiU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFigYgK+zcDVpQmdMYiU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFigYgK+zcDVpQmdMYiU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFigYgK+zcDVpQmdMYiU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFigYgK+zcDVpQmdMYiU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFigYgK+zcDVpQmdMYiU872F9jSfbvOFYyKWrdL	aza nie ące cza zeń, w table  org Filter PL_PGS PL_PGS PL_PGS PL_PGS PL_PGS	e jest szyf asu rozpoz rskaźniki r widoczna modelP Filter Redmi Note 8 Pro Redmi Note 8 Pro Redmi Note 8 Pro Redmi Note 8 Pro Redmi Note 8 Pro	znania, rssi oraz jest po  podelc Filter sM-G920F SM-G920F SM-G920F SM-G920F SM-G920F SM-G920F	rssi Filter -83 -84 -80 -83 -85
	/dat Tabl prot txPo  Table:    Filt   1   125   2   136   3   133   4   132   5   133   6   134   7   58   8   59	a/data/pl.g ica record_ okołu, tem wer. Przykł id timestamp or Filter 1588649544594 1588649685554 1588649832474 1588650272201 1588650272201 15886507722201 15886507141931	table pID, table adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_  msg  Filter xuN9eFSsrrcFigYgK+zcDVpQmdMYiU872F9j5fbvOFYykWrdL xuN9eFSsrrcFigYgK+zcDVpQmdMYiU872F9j5fbvOFYykWrdL xuN9eFSsrrcFigYgK+zcDVpQmdMYiU872F9j5fbvOFYykWrdL xuN9eFSSrrcFigYgK+zcDVpQmdMYiU872F9j5fbvOFYykWrdL xuN9eFSSrrcFigYgK+zcDVpQmdMYiU872F9j5fbvOFYykWrdL xuN9eFSSrrcFigYgK+zcDVpQmdMYiU87ZF9j5fbvOFYykWrdL xuN9eFSSrrcFigYgK+zcDVpQmdMYiU87ZF9j5fbvOFYykWrdL xuN9eFSsrrcFigYgK+zcDVpQmdMYiU87ZF9j5fbvOFYykWrdL wYnzDqmkSw3jM4CJ9nGTpTZmyjrX0bYodd+3ldGXSWDCSN wYnzDqmkSw3jM4CJ9nGTpFTZmyjrX0bYodd+3ldGXSWDCSN	aza niegec cza zeń, w table  arable  a	e jest szyf asu rozpoz zskaźniki r widoczna modelp Filter Redmi Note 8 Pro	znania, ssi oraz jest po modelc Fiter SM-G920F SM-G920F SM-G920F SM-G920F SM-G920F SM-G920F SM-G920F SM-G920F SM-G920F	rssi Filter -83 -84 -80 -83 -85 -82 -80 -79
	/dat Tabl prot txPo  Table:	a/data/pl.g ica record_ okołu, tem wer. Przykł id timestamp ir Filter 1588649635554 1588649932474 1588649923120 15886501681242 158863091899 1588637141931 1588637279711	table pID, table adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_  msg  Filter xuN9eFSsrrcFigYgK+zcDVpQmdMYiU872F9jSfbvOFYyKWrdL wYnzDqmkSw3/l4CL9nGTpFTZmyjrX0bYotd+3ldGXSWDCSN wYnzDqmkSw3/l4CL9nGTpFTZmyjrX0bYotd+3ldGXSWDCSN wYnzDqmkSw3/l4CL9nGTpFTZmyjrX0bYotd+3ldGXSWDCSN	aza niegące cza zeń, w table  table  org  Filter  PLPGS	e jest szyf asu rozpoz rskaźniki r widoczna  rodelP Filter Redmi Note 8 Pro	znania, rssi oraz jest po modelc Filter SM-G920F	rssi Filter -83 -84 -80 -83 -85 -82 -80 -79 -84
	/dat Tabl prot txPo  Table:	a/data/pl.g ica record_ okołu, tem wer. Przykł record_table id timestamp r Filter 1588649534594 1588649932474 1588649923120 1588659168142 158863718193 1588637141931 1588637181780	table pID, table adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_  msg  Filter xuN9eFSsrrcFigYgK+zcDVpOmdMYiU872F9j5fbvOFYykWrdL xuN9eFSsrrcFigYgK+zcDVp	aza niegące czazeń, w table  table  org Filter PLPGS	e jest szyf asu rozpoz zskaźniki r widoczna modelp Filter Redmi Note 8 Pro	znania, ssi oraz jest po modelc Fiter SM-G920F SM-G920F SM-G920F SM-G920F SM-G920F SM-G920F SM-G920F SM-G920F SM-G920F	rssi Filter -83 -84 -80 -83 -85 -82 -80 -79 -84
	/dat Tabl prot txPo  Table:	a/data/pl.g ica record_ okołu, tem wer. Przykł id timestamp ir Filter 1588649635554 1588649932474 1588649923120 15886501681242 158863091899 1588637141931 1588637279711	table pID, table adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_  msg  Filter xuN9eFSsrrcFigYgK+zcDVpQmdMYiU872F9jSfbvOFYyKWrdL wYnzDqmkSw3/l4CL9nGTpFTZmyjrX0bYotd+3ldGXSWDCSN wYnzDqmkSw3/l4CL9nGTpFTZmyjrX0bYotd+3ldGXSWDCSN wYnzDqmkSw3/l4CL9nGTpFTZmyjrX0bYotd+3ldGXSWDCSN	aza nie ące cza zeń, w table  org Filter PL PGS	e jest szyf asu rozpoz rskaźniki r widoczna  rodelP Filter Redmi Note 8 Pro	znania, rssi oraz jest po modelc Filter SM-G920F	rssi Filter -83 -84 -80 -83 -85 -82 -80 -79 -84
	/dat Tabl prot txPo  Table    Filte   1   12     2   136     3   131     4   132     5   134     7   58     8   59     9   60     10   61     11   62	a/data/pl.g ica record_ okołu, tem wer. Przykł  record_table id timestamp ir Filter 1588649544594 1588649544594 1588649832474 1588650168142 1588650168142 158865017141931 15886373141980 1588637381780 1588637381780	table pID, to adow	c.protegosafe/databases. B zawiera informacje dotycza g organizacji, nazwy urząd a zawartość tablicy record_  Big organizacji, nazwy urząd a zawartość tablicy record_  Biter	aza niegece cza zeń, w table  table  filter PLPGS	e jest szyf asu rozpo: rskaźniki r widoczna  modelP Filter Redmi Note 8 Pro	znania, rssi oraz jest po modelc Filter SM-G920F	rssi Filter -83 -84 -80 -85 -82 -80 -79 -84
	/dat Tabl prot txPo  Table:	a/data/pl.g ica record_ okołu, tem wer. Przykł  record_table id timestamp ir Filter 1588649953554 1588649932474 1588649932120 15886501681242 158863918199 1588637121931 1588637121931 1588637217203 1588637717203 1588637717203	table pID, table adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_  msg  Filter xuN9efSsrrcFigYgK+zcDVpCmdMYiU872F9j5fbvOFYykWrdL xuN9efSsrrcFigYgK+zcDVp	aza niegące cza zeń, w table  table  filter PLPGS PLPG	e jest szyf asu rozpoz rskaźniki r widoczna rskaźniki r widoczna  rodelP Filter Redmi Note 8 Pro	znania, rssi oraz jest po modelc Filter SM-G920F	rssi Filter -83 -84 -80 -83 -85 -82 -80 -79 -84 -79 -80 -83 -67 -62
	/dat Tabl prot txPo  Table:	a/data/pl.g ica record_ okołu, tem wer. Przykł  record_table id timestamp ir Filter 1588649544594 1588649544594 1588649582474 1588650168142 1588650168142 1588650171293 1588637381780 1588637381780 1588637712931 1588637712931 1588627417907 1588627417907	table pID, to adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_  imag  ima	aza nie  aza nie  azeń, w table  filter PL PGS	e jest szyf asu rozpo: rskaźniki r widoczna  modelP Filter Redmi Note 8 Pro	znania, rssi oraz jest po modelc Filter SM-G920F	rssi   rssi   Filter   -83   -84   -80   -82   -80   -79   -84   -79   -80   -83   -67   -62   -67   -62   -67   -62   -67   -62   -67   -79   -84   -79   -85   -
	/dat Tabl prot txPo  Table:	a/data/pl.g ica record_ okołu, tem wer. Przykł  d timestamp Filter 1588649544594 1588649584594 158864968554 15886496812474 1588650272291 158863731190 158863731190 158863731190 158863732170 158863732170 158863731190 158863731190 158863731190	table pID, table adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_  imag  ima	aza nie  ace cza zeń, w table  filter PLPGS	e jest szyf asu rozpoz rskaźniki r widoczna rskaźniki r widoczna  rodelP Filter Redmi Note 8 Pro	znania, rssi oraz jest po  modelc Filter SM-G920F	rssi Filter -83 -84 -80 -83 -85 -82 -80 -79 -84 -79 -80 -83 -67 -62
	/dat Tabl prot txPo  Table:	a/data/pl.g ica record_ okołu, tem wer. Przykł  record_table id timestamp ir Filter 1588649544594 1588649544594 1588649582474 1588650168142 1588650168142 1588650171293 1588637381780 1588637381780 1588637712931 1588637712931 1588627417907 1588627417907	ov.mo table pID, to adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_  imag  ima	aza niegece cza zeń, w table  table  filter PLPGS PLPG	e jest szyf asu rozpoz rskaźniki r widoczna  modelP  Filter Redmi Note 8 Pro	znania, rssi oraz jest po modelc Filter SM-G920F	rssi rssi Filter -83 -84 -80 -83 -84 -80 -79 -84 -79 -80 -83 -67 -62 -67 -57
	/dat Tabl prot txPo  Table:	a/data/pl.g ica record_ okołu, tem wer. Przykł id timestamp ir   Filter	table pID, to adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_  imag  ima	aza niegące cza zeń, w _table  filter PLPGS	e jest szyf asu rozpoz rskaźniki r widoczna  modelP Filter Redmi Note 8 Pro	znania, rssi oraz jest po  modelC Fiter SM-G920F	rssi Filter -83 -84 -80 -83 -85 -82 -80 -79 -84 -79 -80 -83 -67 -62 -67 -57
	/dat Tabl prot txPo	a/data/pl.g ica record_ okołu, tem wer. Przykł  d timestamp Filter 158864954594 1588649584594 1588649685554 1588649685554 1588650272291 1588637381780 15886373217971 1588637321790 1588637321790 1588637321790 1588637321790 1588637321790 1588637321790 1588637321790 1588637321790 1588637321790 1588637321790 1588637321790 1588637321790 1588637321790 1588637321790 1588637321790 1588637321790 1588637321790 1588637321790 158864021790 1588640217190	table pID, to adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd ag organizacji, nazwy urząd a zawartość tablicy record_  """  """  """  """  """  """  """	aza nie  ace cza zeń, w table  filter PLPGS	e jest szyf asu rozpo: rskaźniki r widoczna  modelP Filter Redmi Note 8 Pro	rannia, rssi oraz jest po modelc Filter SM-G920F	rssi rssi Filter -83 -84 -80 -79 -84 -79 -80 -67 -62 -67 -57 -61 -79 -80
	/dat Tabl prot txPo  Table:	a/data/pl.g ica record_ okołu, tem wer. Przykł id timestamp or Filter 1588649544594 1588649544594 1588649832474 1588649923120 1588650272291 158863727931180 158863727931180 1588637279014 158862772662 1588627726542 1588627726542 1588627726542 1588627726542 1588627726542 1588627720542 1588627720542 1588627720542 1588627720542 1588627720542 1588627720542 1588627720542 1588640217201 1588640257991 1588640257991	table pID, to adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record a zawartość tablicy record a zawartość tablicy record  i msg  Filter	aza niegece cza zeń, w table  filter pless	e jest szyf asu rozpoz rskaźniki r widoczna modelP Filter Redmi Note 8 Pro	znania, rssi oraz  jest po  modelC  Filter SM-G920F	rssi Filter -83 -84 -80 -83 -85 -82 -80 -79 -84 -79 -61 -79 -80 -81 -79 -81 -79 -81 -79 -82 -79 -81 -79 -82 -79 -81 -79 -79 -81 -79 -81 -79 -79 -81 -81 -79 -81 -81 -79 -81 -81 -81 -81 -81 -81 -81 -81 -81 -81
	/dat Tabl prot txPo  Table:	a/data/pl.g ica record_ okołu, tem wer. Przykł id timestamp ir Filter 1588649832474 1588649832474 1588649832474 1588639689554 158863721911 1588637279110 1588637279110 1588637241931 158863724011 158863726849 158863721911 1588637511931 1588637511931 1588637511931 1588637511931 1588637511931 1588637511931 1588637511931 1588637511931 1588637511931 1588637511931 1588637511931 1588637511931 1588637511931 1588637511931 1588637511931 1588637511931 1588637511931 1588637511931 1588637511931 158863757931	table pID, table adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_  Filter  msg  Filter  xuN9eFSsrrcFigYgK+zcDVpQmdMYiU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFigYgK-zcDVpQmdMYiU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFigYgK-zcDVpQmdMYiU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFigYgK-zcDVpQmdMYiU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFigYgK-zcDVpQmdMYiU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFigYgK-zcDVpQmdMYiU872F9jSfbvOFYyKWrdL xuN9eFSSrrcFigYgK-zcDVpQmdMYiU872F9jSbvOFYyKWrdL xuN9eFSSrrcFigYgK-zcDVpQmdMYiU872F9jSbvOFYyMgMymdTyDqSDplSrvwSzyAkD xuN9ri3Tp+BetlifeTORxkucjusttalljtstrydsYDbskrwsZyAkD xuN9ri3Tp-	aza niegece cza zeń, w table  in org piter plycs	e jest szyf asu rozpoz rskaźniki r widoczna rskaźniki r widoczna rozpoz rskaźniki r widoczna rozpoz rskaźniki r widoczna rozpoz rskaźniki r widoczna rozpoz	znania, rssi oraz jest po modelc Filter SM-G920F	rssi Filter -83 -84 -80 -99 -84 -79 -62 -67 -57 -61 -79 -80 -84 -79 -84
	/dat Tabl prot txPo  Table:	a/data/pl.g ica record_ okołu, tem wer. Przykł id timestamp or Filter 1588649544594 1588649544594 1588649832474 1588649923120 1588650272291 158863727931180 158863727931180 1588637279014 158862772662 1588627726542 1588627726542 1588627726542 1588627726542 1588627726542 1588627720542 1588627720542 1588627720542 1588627720542 1588627720542 1588627720542 1588627720542 1588640217201 1588640257991 1588640257991	table pID, to adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record a zawartość tablicy record a zawartość tablicy record  i msg  Filter	aza nie  azeń, w table  corporation in	e jest szyf asu rozpoz rskaźniki r widoczna modelP Filter Redmi Note 8 Pro	znania, rssi oraz  jest po  modelC  Filter SM-G920F	miżej:  rssi  Filter -83 -84 -80 -83 -85 -82 -80 -79 -84 -79 -86 -67 -57 -61 -79 -80 -84 -79
	/dat Tabl prot txPo  Table	a/data/pl.g ica record_ okołu, tem wer. Przykł  record_table id timestamp ir Filter 1588649544594 1588649544594 1588649582474 1588650272291 1588650168142 1588637279711 1588637279711 1588637279711 1588637279711 1588637279711 1588627827901 158862771200 158862771200 158862771200 158862771200 1588640027791 1588640027791 1588640027791 1588640027791 1588640027791 158864002791 158864002791 158864002791 158864002791 158864002791	cov.mo	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd ag organizacji, nazwy urząd a zawartość tablicy record_  """  """  """  """  """  """  """	aza nie  azeń, w table  arabier  pl.pos	e jest szyf asu rozpo: rskaźniki r widoczna  modelP Filter Redmi Note B Pro	rest po  res	rssi  rssi  Filter -83 -84 -80 -83 -85 -82 -80 -79 -84 -79 -80 -83 -67 -62 -67 -57 -61 -79 -80 -84 -79 -80 -84 -79 -80 -84 -79 -80 -84 -79 -80 -84 -79 -80 -84 -79 -80 -84 -79 -80 -84 -79 -80 -84 -79 -80 -84 -79 -80 -84 -79 -83 -83 -83
	/dat Tabl prot txPo  Table    Filte   1   12   13   13   14   13   13   14   13   13	a/data/pl.g ica record_ okołu, tem wer. Przykł  record_table id timestamp ir Filter 1588649544594 1588649544594 1588649544594 158864952474 1588649832474 1588650272291 158863722191 1588637321791 1588637321790 1588637321790 158862742061 15886277120542 1588627820542 15886277120542 1588627820542 1588627932665 1588640027119 1588640027119 1588640027119 1588640027119 1588640027119 1588640027119 1588640027119 1588640027119 1588640027119 1588640027119	ov.mo table pID, to adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record_  """  """  """  """  """  """  """	aza nie  ace cza  zeń, w  table  filter  pl.pos	e jest szyf asu rozpo: rskaźniki r widoczna  modelP Filter widoczna  modelP Filter Filter Redmi Note 8 Pro	znania, ssi oraz jest po modelc Filter SM-G920F	rssi   Filter   -83   -84   -79   -80   -81   -79   -80   -84   -79   -80   -83   -84   -79   -80   -84   -79   -80   -84   -79   -80   -80   -7
	/dat Tabl prot txPo  Table:	a/data/pl.g ica record_ okołu, tem wer. Przykł  d timestamp ir   Filter	table pID, to adow	c.protegosafe/databases. B zawiera informacje dotycza ag organizacji, nazwy urząd a zawartość tablicy record  """""""""""""""""""""""""""""""""""	aza nie  ace cza  zeń, w table  filter PLPGS	e jest szyf asu rozpo: skaźniki r widoczna  skaźniki r widoczna  modelP  Filter Redmi Note 8 Pro	znania, rssi oraz  jest po  modelc  Filter SM-6920F	miżej:  rssi  Filter -83 -84 -80 -83 -85 -82 -80 -79 -84 -79 -80 -83 -67 -57 -61 -79 -80 -84 -79 -83 -84 -89 -89 -88 -89 -89 -89 -89 -89 -89 -89



#### 6.6. SEQ20200500306

PODATNOŚĆ	[Android] Dane wrażliwe – dane medyczne uzupełnione w trakcie ankiety nie są szyfrowane w pamięci nieulotnej	PRIORYTET	ŚREDNI			
CVSS VECTOR	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	CVSS:3.0 base score	6.5			
OPIS	Aplikacja przechowuje odpowiedzi na pytania w ryzyka zakażenia wraz z wynikiem tej oceny w k mechanizmu WebView (silnika przeglądarki). D w przypadku zainfekowania zrootwanego urzącoprogramowaniem (lub zainfekowania dowoln oprogramowaniem posiadającym funkcjonalno prowadzić do ujawnienia danych medycznych a	okalnej pamię vane te nie są s dzenia złośliwy ego urządzeni sść rootowania	ci (local storage) szyfrowane, co vm a złośliwym			
ZALECENIA	Zaszyfrować wrażliwe dane znajdujące się w /data/data/pl.gov.mc.protegosafe/app_webview/Default/Local Storage/leveldb.					
SZCZEGÓŁY TECHNICZNE	Aplikacja dla Android przechowuje odpowiedzi dotyczącej oceny ryzyka zakażenia wraz z wynił pamięci, w pamięci lokalnej mechanizmu Weby baza danych LevelDB znajdujące się w katalogu /data/data/pl.gov.mc.protegosafe/app_webvie Storage/leveldb. Przykładowa zawartość bazy o 'app': '{"onboardingFinished":true,"startScreenShowed":true} 'diagnosis': '{"evidence":[],"inProgress":false,"isLoading":false,"isResetting 'triage': '{"isLoading":false,"triageLevel":"no_risk","label":"Po epidemiologicznymi.","description":"Odpowiedzi, których udz koronawirusem (choroba COVID-19). Stosuj poni sze [rodki za Pamitaj,  e Twoje objawy mog wynika tak e z innych chorób i powy szy wywiad jest ukierunkowany na COVID-19. Je[li twoje si z lekarzem.","serious":[]}', 'user': '{"age":29,"bloodGroup":"B+","chronicSicks":[],"name":"Aaa",  ""id":"p_15","choice_id":"present"}],"triageLevel":"no_risk","lepidemiologicznymi.","description":"Odpowiedzi, których udz koronawirusem (choroba COVID-19). Stosuj poni sze [rodki za Pamitaj,  e Twoje objawy mog wynika tak e z innych chorób i powy szy wywiad jest ukierunkowany na COVID-19. Je[li twoje si z lekarzem."}}', 'daily': '{"1588586778":{"data":{"temperature":36.5,"runnyNotaliy:'"1588586778":{"data":"temperature":36.5,"runnyNotaliy:'"1588586778":{"data":"temperature":36.5,"runnyNotaliy:'"11,"chills":"level 1","musclePain":"level 1","contacts":""}}}',	kiem tej oceny View, zaimpler Lew/Default/Lo danych widocz  ", g":true,"question":{ stpuj zgodnie z zale ieliBe[, nie wskazuj pobiegawcze, by ur mog wymaga konsu e objawy wydaj si ni "sex":"male","smol abel":"Postpuj zgoc ieliBe[, nie wskazuj pobiegawcze, by ur mog wymaga konsu e objawy wydaj si ni	mentowanej jako  cal na jest poniżej:  },"allQuestions":[]}', ceniami na zaka enie nikn zaka enia. ultacji lekarskiej - epokojce, skontaktuj  keNumber":null}',  lnie z zaleceniami na zaka enie nikn zaka enia. ultacji lekarskiej - epokojce, skontaktuj			



#### 6.7. SEQ20200500307

PODATNOŚĆ	[iOS] Dane wrażliwe – zawartość pliku plist z listą tempID nie jest szyfrowana w pamięci nieulotnej	PRIORYTET	ŚREDNI
CVSS VECTOR	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	CVSS:3.0 base score	6.5
OPIS	Tymczasowe identyfikatory utrzymywane są ni /var/mobile/Containers/Data/Application/APP UUID/Library/Preferences/pl.gov.mc.protegoso uzyska dostęp do systemu plików na urządzeni identyfikatory, które użytkownik rozgłasza i bęczasie.	- n <i>fe.plist</i> . Ataku u może pozysk	jący, który ać
ZALECENIA	Zalecamy wprowadzenie mechanizmu jailbreak problem dostępu do wrażliwych danych na jaill Zalecamy przechowywać tymczasowe identyfik	breakowanych	urządzeniach.
SZCZEGÓŁY TECHNICZNE	Tymczasowe identyfikatory znajdują się w pliku w lokalizacji /var/mobile/Containers/Data/App UUID/Library/Preferences pod kluczem BROAD BROAD_MSG_ARRAY:  {     "ADVT_DATA" = {length = 128, bytes = 0x7b226d70 223a2269 50686f6e 223a327d };     "ADVT_EXPIRY" = "2020-05-11 00:26:43 +0000";     "BROADCAST_MSG" = "HeVc6nqmQj1h/vmlEaRalJIIS/awzroLJGbVjDY9R8QYR0FPjOvBCx6oDzml/s" = ";     "BROAD_MSG_ARRAY" = {	e 65205822 222c227  AVFFG611lkuQUfM5QV  LkH6uZudKMU/mBtLEY	az 6 /100g= /q8FFgr



#### 6.8. SEQ20200500308

PODATNOŚĆ	zav	νie	erają	ca li	stę (	-	tan	ych te	ych empID, i lotnej	nie	PRIORYTET	ŚREDNI	
CVSS VECTOR	AV	:N,	/AC:I	_/PR	:L/U	II:N/S	:U/0	C:H/I:	N/A:N		CVSS:3.0 base score	6.5	
OPIS	są /vc /vc Sup urz his	w i ar/i opo ad tor	niesz mobi ort/ti zeni	yfro ile/C race u mo ntak	wan conto r.sq oże p ctów	nej ba: giners lite. A pozys	zie ( /Da takı kać	danyo nta/A <sub>l</sub> ujący, ident	ch oplication który u cyfikator	on/APP_ zyska d y uzysk	nych urządzeń _ <i>UUID/Librar</i> y ostęp do syst ując informac urządzeniami i	//Application emu plikóv ije dotyczą	on v na ce
ZALECENIA			•	•					•		k-detection, k breakowanych	, ,	•
	Zal	ec	amy	zast	oso\				ania baz				
SZCZEGÓŁY TECHNICZNE	Zal Baz /va Suj wp	za : ar/i ppo	sqlite mobi ort. E	zast e tra ile/C Baza w pr	cer.	sqlite ainers jest s	zna /Da zyfr wer	ajduje ata/A <sub>l</sub> owan sji An	się w lo oplicatio a. Tablio droid. P	okalizac on/APP- ca ZEN(		iera podob	
	Zal Baz /va Suj wp	za : ar/i ppo oisy NC	sqlite mobi ort. E	zast e tra ile/C Baza w pr	cer.	sqlite ainers jest sa adku v	zna /Da zyfr wer	ajduje ata/A <sub>l</sub> owan sji An	się w lo oplicatio a. Tablio droid. P	okalizac on/APP- ca ZEN(	ji -UUID/Library COUNTER zaw	iera podok ść tablicy	
	Baz /va Sul wp ZEI	za : ar/i ppo oisy NC	sqlite mobi ort. E	zast e tra ile/C Baza w pr TER	cer. containie rzypa	sqlite ainers jest sa adku v oczna	zna s/Da zyfr wer	ajduje ata/A <sub>l</sub> owan sji An	się w lo oplicatio a. Tablio droid. P iiżej:	okalizac on/APP- ca ZEN(	ji -UUID/Library COUNTER zaw owa zawartos	iera podok ść tablicy	one
	Baz /va Sul wp ZEI	za : ar/i ppo oisy NC	sqlite mobi ort. E gjak OUN	zast e tra ile/C Baza w pr TER	cer. conta	sqlite ainers jest s adku v oczna	zna s/Da zyfr wer i jes	ajduje ata/Al owan sji An st pon	się w lo oplicatio a. Tablio droid. P iiżej:	okalizac on/APP- ca ZEN( Przykład	ji -UUID/Library COUNTER zaw owa zawartos	iera podok ść tablicy	one
	Baz /va Sul wp ZEI	za : ar/i ppo oisy NC	sqlite mobi ort. E gjak OUN	zast e tra ile/C Baza w pr TER	cer. containie zypa wid	sqlite ainers jest s: adku v oczna	zna s/Da zyfr wer i jes	ajduje ata/Ap owan sji An st pon	się w lo oplicatio na. Tablio droid. P niżej:	okalizac on/APP- ca ZEN( rzykład	ji -UUID/Library COUNTER zaw owa zawartos	iera podok ść tablicy	ord Delete Record
	Baz /va Sul wp ZEI	za : ar/i ppo oisy NC	sqlite mobi ort. E gjak OUN	zast e tra ile/C Baza w pr TER	cer. Contanie zypa wid	sqlite ainers jest s: adku v oczna	zna zna zyfr zyfr wer i jes	ata/Aprowan sji An st pon Filter MILLE MILLE MILLE Phone X	się w lo oplicatio na. Tablio droid. P niżej:	okalizac on/APP- ca ZEN( Przykład	ji -UUID/Library COUNTER zaw owa zawartoś	iera podok ść tablicy  New Rec	Delete Record  ZORG  Filter  NVLL  PLPGS  PLPGS
	Baz /va Sul wp ZEI	za : ar/i ppo oisy NC	sqlite mobi ort. E gjak OUN	zast e tra ile/C Baza w pr TER	cer. containie zypa wid	sqlite ainers jest s: adku v oczna	zna zna zyfr zyfr wer i jes	ajduje ata/Ap cowan sji An st pon	się w lo oplicatio a. Tablio droid. P liżej:	okalizac on/APP- ca ZENC Przykład	ji -UUID/Library COUNTER zaw owa zawartoś	iera podok ść tablicy  New Rec	Delete Record  ZORG  Filter  NULL  PL_PGS
	Baz /va Sul wp ZEI	za : ar/i ppo oisy NC	sqlite mobi ort. E gjak OUN	zast e tra ile/C Baza w pr TER	cer. containie zypa wid  zass pit	sqlite ainers jest si adku v oczna  t zimestam filler 61044231. 61044236. 61044224. 61044224.	zna s/Da zyfr wer jes	ajduje ata/Aprowan sji An sji An st pon  /EF 2MODELC   Pitter   NULL   Pitter	się w lopolicatico poplicatico	pikalizac pn/APP- ca ZENC erzykład Fitter scanning started fr4p/GoskijhLZEW scanning stoped scanning stoped fr4p/GoskijhLZEW	ji -UUID/Library COUNTER zaw owa zawartoś  ZMSG  ZMSG  ZMSG  ZMSG  ZMSG  ZMSG  ZMSG	New Rec	DINE  Delete Record  ZORG  Filter  AMULL  PL PGS  MULL  PL PGS
	Baz /va Sul wp ZEI	za : ar/i ppo oisy NC	sqlite mobi ort. E gjak OUN	zast e tra ile/C Baza w pr TER	cer. containie zypa wid	sqlite ainers jest s. adku v oczna  i zimestam filter 610444230. 610444231. 61044231.	zna s/Da zyfr wer i jes i jes i lo. o. o	ajduje ata/Ap owan sji An st pon filter phone x piphone x pikkl	się w lo oplicatio a. Tablio droid. P iiżej:	pikalizac pn/APP- ca ZENC erzykład Fitter scanning started fr4p/GoskijhLZEW scanning stoped scanning stoped fr4p/GoskijhLZEW	ji -UUID/Library COUNTER zaw owa zawartoś zwsci	New Rec	DINE  Delete Record  ZORG  Filter  AMULL  PL PGS  MULL  PL PGS
	Bai /va Sul wp ZEI	eca	sqlite mobi ort. E gjak OUN	zast  e tra  e tra  gaza  w pr  TER  TER   must  a 2  a 2  a 2  a 3  must  mus	ZRSS   Filt.   .	sqlite ainers jest si adku v oczna  t zillestaku si oczna  t zillestaku si olakazai 610442231. 61044224. 61044224. 61044224. 61044224. 61044231. 61044231. 61044231.	znazyfrweri jes	ajduje ata/Ap rowan sji An st pon filter place p	się w lopplicationa. Tablio droid. Poliżej:    ZMODELP   Filter   MIELE   MIEL	PRICE PROCESSING STATES	ji -UUID/Library COUNTER zaw owa zawartoś  zwsc  zwsc  iboyvejoxitzlime4us1YF2VCysddztx chkljop8HMAKFZUm65zArpvVIBdCQs:	New Rec  +92FXB2Qzc13ELpPdegwtrQ  +92FXB2Qzc13ElpPdegwtrQ  +92FXB2Qzc13ElpPdegwtrQ  +92FXB2Qzc13ElpPdegwtrQ	DINE  ZORG  Filter  AUALL  PILPGS  PILPGS  PLPGS  PLPGS  RUALL  RUALL  RUALL
	Bai /va Sup wp ZEI	za: ar/i ppo isy VC	amy sqlite mobi  ort. E  jak  OUN	zast e tra ile/C 3aza w pr TER  TER  AUGUST  A	Cer. Conta nie zypa wid zrszypa wid zrszyp	sqlite ainers jest s: adku v oczna    ZIIMESTAM   FILOP   FILO	zna zna zyfr  wer  jess  i jes	ajduje ata/Ap owan sji An st pon filter MALL Phone X MALL Phone X MALL MALL Phone X	się w lo oplicatio a. Tablio droid. P iiżej:    ZMODELP   Filter   MAILL   MAILL   MAILL   SSH-0920F   Redmi Note 8 Pro   Redmi	PROGOSHUNLZEW PROGOSHUNLZEW PROGOSHUNLZEW PROGOSHUNLZEW PROGOSHUNLZEW PROGOSHUNLZEW PROGOSHUNLZEW PROGOSHUNLZEW PROGOSHUNLZEW	ji -UUID/Library COUNTER zaw owa zawartoś zwsc  zwsc iboyvwjoxtizlime4u/s1YF2VCysddzix chk1joP8HMAKF2Umt65zArpvWlBdCQs:	New Reci +92FXB2Qzc13ELpPdegwtrQ +92FXB2Qzc13ELpPdegwtrQ +92FXB2Qzc13ELpPdegwtrQ 104zm+/5MC12wRp2Q/139Hk 104zm+/5MC12wRp2Q/139Hk	DONG  Delete Record  ZORG  Filter  FILTER  FILTER  PL PGS  PL PGS  PL PGS  PL PGS  AMALL  MALL  PL PGS
	Baz /va Sul wp ZEI	eca	amy sqlite mobi	zast  e tra  e tra  gaza  w pr  TER  TER   must  a 2  a 2  a 2  a 3  must  mus	ZRSS   Filt.   .	sqlite ainers jest si adku v oczna  t zillestaku si oczna  t zillestaku si olakazai 610442231. 61044224. 61044224. 61044224. 61044224. 61044231. 61044231. 61044231.	znazyfrweri jes	ajduje ata/Ap rowan sji An st pon filter place p	się w lo oplicatio a. Tablio droid. P iiżej:  ZMODELP FILET SM-0920F Redmi Note 8 Pro MALL SM-0920F Redmi Note 8 Pro MALL Redmi Note 8 Pro	PROGOSHUNLZEW PROGOSHUNLZEW PROGOSHUNLZEW PROGOSHUNLZEW PROGOSHUNLZEW PROGOSHUNLZEW PROGOSHUNLZEW PROGOSHUNLZEW PROGOSHUNLZEW	ji -UUID/Library COUNTER zaw owa zawartoś  zwsc  zwsc  iboyvejoxitzlime4us1YF2VCysddztx chkljop8HMAKFZUm65zArpvVIBdCQs:	New Reci +92FXB2Qzc13ELpPdegwtrQ +92FXB2Qzc13ELpPdegwtrQ +92FXB2Qzc13ELpPdegwtrQ 104zm+/5MC12wRp2Q/139Hk 104zm+/5MC12wRp2Q/139Hk	DINE  ZORG  Filter  AUALL  PILPGS  PILPGS  PLPGS  PLPGS  RUALL  RUALL  RUALL
	Bail /va Sup wp ZEI  Jable:  1 2 3 4 5 6 7 8 9 10 11 12 13	Za: za: za: zar/I ppo pisy NC  zenc z pk z 1	amy sqlite mobi	zast e tra ile/C 33aza w pr TER  TER  DPT ZV 2 2 1 MALL 2 2 1 MALL 4 MAL	ZRSS   Filt.   Sl. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.	sqlite ainers jest s: adku v oczna  4 ziimestam filter 61044230. 61044231. 61044231. 61044231. 61044235. 61044352. 61044352. 61044352.	zna s/Da s/Da zyfr wer i jes i jes i lo	ajduje ata/Ap owan sji An st pon st pon filter NULL iPhone X iPhone X iPhone X NULL iPhone X	się w lo oplicatio a. Tablio droid. P iiżej:    ZMODELP   Filter   NULL   SM-0320F   Radmi Note 8 Pro   MULL   NULL   SM-0320F   Radmi Note 8 Pro   Radmi Note	Pilter Scanning started fraprioacyjiarus Procoshujhuzew Scanning started fraprioacyjiarusw Procoshujhuzew Scanning started fraprioacyjiarusw Scanning started Fraprioacyjiarusw Scanning started	JI  -UUID/Library COUNTER zaw owa zawartoś  ZMSG  IGOYWIJAZIZIIIm64u/31YF2VCysGdZIX (IGOYWIJAZIZIIIm64u/31YF2VCysGdZIX (IRL)JPBHMAKFZUm165ZArpwVIBdCQs;  IRL)JPBHMAKFZUm165ZArpwVIBdCQs;  (IRL)JPBHMAKFZUm165ZArpwVIBdCQs;	New Rec  +92FXB2Q2c13ELpPdegwtrQ  +92FXB2Q2c13ELpPdegwtrQ  192FXB2Q2c13ELpPdegwtrQ  194zm+/5MC12wRp2Q/139Hk  194zm+/5MC12wRp2Q/139Hk  194zm+/5MC12wRp2Q/139Hk	DINE  Delete Record  ZORG  Filter  FILER  PL_PGS  PL_PGS  AMALL  MALL  PL_PGS  AMALL  MALL  PL_PGS  AMALL  MALL  REALL  REALL  REALL  MALL
	Zal Baa /va Sul wp ZEI  Jable  1 2 3 4 5 6 7 8 9 10 11 12 13 14	Za: za: za: ppo pisy NC  zenc zenc zenc zenc zenc zenc zenc zen	amy sqlite mobi prt. E OUN  OUN  I I I I I I I I I I I I I I I I I I	zast e tra ille/C 3aza w pr TER  TER  AMAL 2 2 2 4MAL 2 2 2 4MAL 2 2 2 4MAL 4MAL 2 4MAL 4MAL 4MAL 4MAL 4MAL 4MAL 4MAL 4MAL	Contain   Cont	sqlite ainers jest s.; adku v oczna <sup>4</sup> Zillestaku v oczna <sup>6</sup> 10444230. 610442421. 61044242. 61044242. 61044232. 61044232. 61044350. 61044350. 61044350.	zna s/Da s/Da s/Da syfr wer i jes ii	ajduje ata/Ap rowan siji An st pon st pon st pon place i place x place	się w lopplication a. Tablie droid. Poliżej:  ZMODELP Filter AMALL SM-0920F Redmi Note 8 Pro AMALL Redmi Note 8 Pro AMALL Redmi Note 8 Pro SM-0920F Redmi Note 8 Pro SM-0920F Redmi Note 8 Pro AMALL Redmi Note 8 Pro SM-0920F	PRGGSShuhLzew Scanning started fr4p/fG8Kyliafuriw PRGGShujhLzew Scanning started fr4p/fG8Kyliafuriw PRGGShujhLzew Scanning started fr4p/fG8Kyliafuriw Fr4p/fG8Kyliafu	ji -UUID/Library COUNTER zaw owa zawartoś zwsc  zwsc iboyvwjoxtizlime4u/s1YF2VCysddzix chk1joP8HMAKF2Umt65zArpvWlBdCQs:	New Rec  New	DINE  ZORG  Filter  MULL  PL POS  PL POS  PL POS  PL POS  PL POS  PL POS  MULL  MULL  MULL  MULL  MULL  MULL  MULL  PL POS  PL POS  PL POS  PL POS  MULL  MU
	Zal Bai /va Sul wp ZEI  Indite: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	Za: za: zar/I  ppo isy  NC  zenc  zenc  zenc  in i	amy sqlite mobi port. E y jak v  OUN  I I I I I I I I I I I I I I I I I I	zast e tra ile/C 3aza w pr TER  TER 2 nnac nnac nnac nnac nnac 2 2 2 nnac nnac	ZRSS   Wid   ZRS	sqlite ainers jest si adku v Oczna  1 ZTIMESTAM FILLER 610444231. 61044221. 61044221. 61044221. 61044221. 61044236. 61044350. 61044350.	znazyfr zyfr wer i jes  Fitter	ajduje ata/Ap rowan sji An st pon filter NULL iPhone X iP	Się w lo pplicatic a. Tablic droid. P iiżej:  ZMODELP Filter NULL SM-G920F Redmi Note 8 Pro NULL SM-G920F Redmi Note 8 Pro NULL SM-G920F Redmi Note 8 Pro NULL Redmi Note 8 Pro NULL Redmi Note 8 Pro NULL Redmi Note 8 Pro	PRGGSShuhLzew Scanning started fr4p/fG8Kyliafuriw PRGGShujhLzew Scanning started fr4p/fG8Kyliafuriw PRGGShujhLzew Scanning started fr4p/fG8Kyliafuriw Fr4p/fG8Kyliafu	ji -UUID/Library COUNTER zaw owa zawartoś  zwsc  zwsc  zwsc  iDoywijoxtizflim64uis1YF2VCysddZix chi.joParMAXFZUmt65zArpvWllbdCosi	New Rec  New	DINE  ZORG  Filter  MULL  PL POS  PL POS  PL POS  PL POS  PL POS  PL POS  MULL  MULL  MULL  MULL  MULL  MULL  MULL  PL POS  PL POS  PL POS  PL POS  MULL  MU
	Zal  Baa: /va Sul wp ZEI  Table 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17	ZENC ZENC ZENC ZENC ZENC ZENC ZENC ZENC	amy sqlite mobi prt. E r jak ' OUN	zast  tra ille/C  3aza  w pr  TER  TER  2  MALL 2 2  MALL 2 2  MALL 4	Z8552 wid  Z8552 wid  Z8552 0.0	sqlite ainers jest si adku v oczna  1 zintestam ritter 610444230. 61044230. 61044230. 61044231. 61044231. 61044231. 61044361. 610444361. 610444361. 610444410. 610444410.	znazyfr zyfr wer jes ' (TXPOW ) - (TXPOW ) - (10	ajduje ata/Ap cowan sji An sji An st pon  //E	Się w lo pplicatic a. Tablic droid. P liżej:  ZMODELP Filter NURLL SM-G920F Redmi Note 8 Pro NURLL SM-G920F Redmi Note 8 Pro SM-G920F Redmi Note 8 Pro SM-G920F NURLL SM-G920F NURLL NURLL SM-G920F NURLL NURL NUR	Pilter Scanning started fr4p/foskylarurw PRGoshulpt.Zew Scanning started fr4p/foskylarurw PRGoshulpt.Zew Scanning started fr4p/foskylarurw PRGoshulpt.Zew Scanning stoped Scanning stoped Scanning started PRGoshulpt.Zew Scanning started	JI  -UUID/Library  COUNTER zaw  Owa zawartoś  ZNSG  ZNSG  ZNSG  ZNSG  LDQyWijxXIIZflim64us1YF2VCysGdZIX  (thk1joPBHMAXFZUmt65zArpvWlBdCQs:  thk1joPBHMAXFZUmt65zArpvWlBdCQs:  (thk1joPBHMAXFZUmt65zArpvWlBdCQs:  LDQyWijxXIIZflim64us1YF2VCysGdZIX  (thk1joPBHMAXFZUmt65zArpvWlBdCQs:  LDQyWijxXIIZflim64us1YF2VCysGdZIX  (thk1joPBHMAXFZUmt65zArpvWlBdCQs:  LDQyWijxXIIZflim64us1YF2VCysGdZIX	New Rec  New	DINE  JORG  JORG  Filter  AUGUL  PL. POS  PL. POS  AUGUL  AUGUL  PL. POS  AUGUL  AUGUL  AUGUL  PL. POS  AUGUL  AUG
	Zal  Bai: /va  Sup wp ZEI  Table:  1 2 3 4 5 6 7 8 9 9 10 11 11 12 13 14 15 16 17 18	22a : 2	amy sqlite mobi port. E  jak  OUN  OUNTER  L  L  L  L  L  L  L  L  L  L  L  L  L	zast e tra ile/C 33aza w pr TER  Pr RIBER 2 2 2 RAGEL 3 RAGEL 3 RAGEL 4 RA	ZRSS   Filt.   SR.0   O.0	sqlite ainers jest s: adku v oczna  4 zīlmēstam filter 610444230. 610444231. 610444231. 610444231. 610444350. 610444350. 610444350. 610444350. 610444350.	zna s/Da s/Da s/Da s/Da s/Da s/Da s/Da s/D	ajduje ata/Ap owan sji An st pon fiter MULL iPhone X	Się w lo pplicatio a. Tablio droid. P iiżej:    ZMODELP     Filter   MAILL   Radmi Note 8 Pro   MAILL   MAILL   Radmi Note 8 Pro   MAILL   MAILL   Radmi Note 8 Pro   MAILL	PROGSHIJLZEW Scanning started	ji -UUID/Library COUNTER zaw owa zawartoś  zwsc  zwsc  zwsc  iDoywijoxtizflim64uis1YF2VCysddZix chi.joParMAXFZUmt65zArpvWllbdCosi	New Reci +92FXB2Q2c13ELpPdegwtrQ +92FXB2Q2c13ELpPdegwtrQ +92FXB2Q2c13ELpPdegwtrQ 104zm+/5MC12wfp2Q/139Hk +92FXB2Q2c13ELpPdegwtrQ  204zm+/5MC12wfp2Q/139Hz +92FXB2Q2c13ELpPdegwtrQ +92FXB2Q2c13ELpPdegwtrQ +92FXB2Q2c13ELpPdegwtrQ	DINE  JORG  Filter  ZORG  Filter  FILPOS  MULL
	Zal  Bai /va Sul wp ZEI  Table:  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20	Za : 2	amy sqlite mobi port. E y jak v  OUN	zast e tra ille/C 3aza w pr TER  TER  MALL 2 2 MALL 2 MALL 2 2 MALL 2 MAL	ZASS   Filt   O.0	sqlite ainers jest si adku v oczna  1 zillesta 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044351. 610444351. 610444351. 610444351. 610444351. 610444351.	zna s/Da s/Da syfr wer i jes crxpow i	ajduje ata/Ap cowan sji An st pon filter pilter pil	Się w lo pplicatic a. Tablic droid. P liżej:    ZMODELP     Filter   NARIA   N	Pilter Scanning started fr4p/Goskyilarurw PRGoshulh.Zepw Scanning started fr4p/Goskyilarurw PRGoshulh.Zepw Scanning started fr4p/Goskyilarurw PRGoshulh.Zepw Scanning started fr4p/Goskyilarurw PRGoshulh.Zepw Scanning started fr4p/Goskyilarurw Scanning started fr4p/Goskyilarurw PRGoshulh.Zepw Scanning started fr4p/Goskyilarurw FRGoshulh.Zepw Scanning stopped Scanning started fr4p/Goskyilarurw FRGoskyilarurw Scanning stopped Scanning started fr4p/Goskyilarurw Scanning stopped Scanning started fr4p/Goskyilarurw Scanning stopped	JI  -UUID/Library COUNTER zaw Owa zawartoś  zwsc  zwsc  idoyvwj.xxtizlim64u/s1YF2VCysddzix chk.j.pPBMAXFZUm65zArpvWlBdCQs;  chk.j.pPBMAXFZUm64s/spYF2VCysGdZix  chk.j.pPBMAXFZUm64s/spYF2VCysGdZix  chk.j.pPBMAXFZUm64s/spYF2VCysGdZix	New Reci +92FXB2Q2c13ELpPdegwtrQ +92FXB2Q2c13ELpPdegwtrQ +92FXB2Q2c13ELpPdegwtrQ 104zm+/5MC12wfp2Q/139Hk +92FXB2Q2c13ELpPdegwtrQ  204zm+/5MC12wfp2Q/139Hz +92FXB2Q2c13ELpPdegwtrQ +92FXB2Q2c13ELpPdegwtrQ +92FXB2Q2c13ELpPdegwtrQ	DINE  Delete Record  ZORG  Filter  AUALL  PL PGS  AUALL  AUALL  AUALL  PL PGS  AUALL  AUALL  PL PGS  AUALL  AUALL  PL PGS  AUALL  AUALL
	Zal  Bai: /va  Sup wp ZEI  Table:  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 15 16 17 18 19 20 21	Za:  Zar/I  ppo  isy  NC  ZENC  ZENC  ZENC  1 1 7 1 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	amy sqlite mobi  ort. E  jak  OUN   ounter  in  in  in  in  in  in  in  in  in  i	zast e tra ile/C 3aza w pr TER  DPT ZV PR	ZRSS   Filt.   SR.0   O.0	sqlite ainers jest si adku v oczna  4 ziihestam filter 61044230. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044431. 61044431. 61044431.	zna s/Da zyfr wer jes   tixpow   tixpow	A MALL  IPhone X  IP	Się w lo pplicatio a. Tablio droid. P iiżej:    ZMODELP     Filter     Filter	Filter Scanning started frapficaskjilarurw Scanning started frapficaskjilarurw PRGGANULTEW Scanning started Scanning started frapficaskjilarurw Scanning started FRGGANULTEW Scanning started FRGGANULTEW Scanning stopped Scanning started FRGGANULTEW Scanning started FRGGANULTEW Scanning started FRGGANULTEW Scanning started FRGGANULTEW Scanning started	JI  -UUID/Library COUNTER zaw owa zawartoś  zwsc  zwsc  iDoywijantz/lim64ws1YF2vCysGdZIX  ikh.joPBIMAXFZUmt65zArpwilBdCqs;  ikh.joPBIMAXFZUmt65zArpwilBdCqs;  ikh.joPBIMAXFZUmt65zArpwilBdCqs;  ikh.joPBIMAXFZUmt65zArpwilBdCqs;  idoywijantz/lim64ws1YF2vCysGdZIX	New Rec  +92FXB2Qzc13ELpPdegwtrQ  +92FXB2Qzc13ELpPdegwtrQ  154zm+/5MC12wRpZ0/139Hk  192FXB2Qzc13ELpPdegwtrQ  154zm+/5MC12wRpZ0/139Hk  192FXB2Qzc13ELpPdegwtrQ  154zm+/5MC12wRpZ0/139Hk  192FXB2Qzc13ELpPdegwtrQ  192FXB2Qzc13ELpPdegwtrQ	DINE  Delete Record  ZORG  FIRET  FILES  PL_PGS  PL_PGS  MALL  MALL  PL_PGS  MALL  MALL  MALL  PL_PGS  MALL
	Zal  Baa: /va  Sul wp  ZEI  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22	Za : 2	amy sqlite mobi prt. E  ount  ount  in  in  in  in  in  in  in  in  in	zast e tra ille/C 3aza w pr TER  TER  MALL 2 2 MALL 2 MALL 2 2 MALL 2 MAL	ZASS   Filt   O.0	sqlite ainers jest si adku v oczna  1 zillesta 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044231. 61044351. 610444351. 610444351. 610444351. 610444351. 610444351.	zna s/Da s/Da syfr wer jes jes illo illo illo illo illo illo illo ill	ajduje ata/Ap cowan sji An st pon filter pilter pil	Się w lo pplicatic a. Tablic droid. P liżej:    ZMODELP     Filter   NARIA   N	Filter Scanning started frapt/Geklyilarurw PRGGoShujhLZEW Scanning started frapt/Geklyilarurw PRGGoShujhLZEW Scanning started frapt/Geklyilarurw FRGGOShujhLZEW Scanning started PRGGOShujhLZEW Scanning started PRGGOShujhLZEW Scanning started PRGGOShujhLZEW Scanning started FRGGOShujhLZEW Scanning started FRGGOShujhLZEW Scanning started FRGGOShujhLZEW Scanning started	JI  -UUID/Library COUNTER zaw Owa zawartoś  zwsc  zwsc  idoyvwj.xxtizlim64u/s1YF2VCysddzix chk.j.pPBMAXFZUm65zArpvWlBdCQs;  chk.j.pPBMAXFZUm64s/spYF2VCysGdZix  chk.j.pPBMAXFZUm64s/spYF2VCysGdZix  chk.j.pPBMAXFZUm64s/spYF2VCysGdZix	New Rec  P92FXB2Ozc13ELPPdegwtrO.  8r4zm+/5MC12wRpZ0/139Hk.  92FXB2Ozc13ELPPdegwtrO.  8r4zm+/5MC12wRpZ0/139Hk.  92FXB2Ozc13ELPPdegwtrO.  8r4zm+/5MC12wRpZ0/139Hk.  92FXB2Ozc13ELPPdegwtrO.  8r4zm+/5MC12wRpZ0/139Hk.  92FXB2Ozc13ELPPdegwtrO.  92FXB2Ozc13ELPPdegwtrO.  92FXB2Ozc13ELPPdegwtrO.  92FXB2Ozc13ELPPdegwtrO.  92FXB2Ozc13ELPPdegwtrO.  92FXB2Ozc13ELPPdegwtrO.	DINE  Ord Delete Record  ZORG Filter  AWALL
	Zal  Baa: /va  Sul wp ZEI  Jabic  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24	220 : 220 : 27 : 27 : 27 : 27 : 27 : 27	amy sqlite mobi ort. E oute oute i i i i i i i i i i i i i i i i i i i	zast  tra ille/C  Baza  w pr  TER  TER  2  MALL  AULI	Cer. Contain nie zypa wid zassa wid zassa wid zassa wid zassa wid zasa wid	sqlite ainers jest si adku v oczna  4 zīimtēstam friter 610444231. 610444231. 610444231. 610444231. 610444351. 610444351. 610444351. 610444431. 610444431. 610444431. 610444431. 610444431. 610444431. 610444431.	zna s/Da zyfr wer i jes  - ETXPOW   Filter   0.0	ANDLE Phone X  NOLL Phone X	SIĘ W ICO DICATIC  DIPLICATIC  ALICA  ALICA  SILONO  FILTE  FAMULE  AMULE  SM-0920F  Redmi Note 8 Pro  SM-0920F  FILTE  FILT	Pitter Scanning started frap/foskylarurw Scanning started frap/foskylarurw Procoshulyhuzew Scanning started frap/foskylarurw Scanning started procoshulyhuzew Scanning stopped	JI  -UUID/Library  COUNTER zaw  Owa zawartoś  ZM5G  ZM5G  ZM5G  ZM5G  ZM5G  ID0yWijoxttzflim64u/s1YF2VCysGdZIX  chk.ljoParMAXFZUmt65zArpvWll8dCqs:  chk.ljoParMAXFZUmt65zArpvWll8dCqs:  (chk.ljoParMAXFZUmt65zArpvWll8dCqs:  Librywijoxttzflim64u/s1YF2VCysGdZIX  chk.ljoParMAXFZUmt65zArpvWll8dCqs:  Librywijoxttzflim64u/s1YF2VCysGdZIX  chk.ljoParMAXFZUmt65zArpvWll8dCqs:  Librywijoxttzflim64u/s1YF2VCysGdZIX  chk.ljoParMAXFZUmt65zArpvWll8dCqs:  Librywijoxttzflim64u/s1YF2VCysGdZIX  chk.ljoParMAXFZUmt65zArpvWll8dCqs:  Chk.ljoParMAXFZUmt65zArpvWll8dCqs:  Chk.ljoParMAXFZUmt65zArpvWll8dCqs:  Chk.ljoParMAXFZUmt65zArpvWll8dCqs:  Chk.ljoParMAXFZUmt65zArpvWll8dCqs:	New Rec  P92FXB2Ozc13ELPPdegwtrO.  8r4zm+/5MC12wRpZ0/139Hk.  92FXB2Ozc13ELPPdegwtrO.  8r4zm+/5MC12wRpZ0/139Hk.  92FXB2Ozc13ELPPdegwtrO.  8r4zm+/5MC12wRpZ0/139Hk.  92FXB2Ozc13ELPPdegwtrO.  8r4zm+/5MC12wRpZ0/139Hk.  92FXB2Ozc13ELPPdegwtrO.  92FXB2Ozc13ELPPdegwtrO.  92FXB2Ozc13ELPPdegwtrO.  92FXB2Ozc13ELPPdegwtrO.  92FXB2Ozc13ELPPdegwtrO.  92FXB2Ozc13ELPPdegwtrO.	DINE  Delete Record  ZORG  Filter  FILPOS  PLPOS  MALL  MALL
	Zal  Baa: /va  Sul wp  ZEI  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25	Za: Zar/I  ppo  isy  CZENC  Z PK Z  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	amy sqlite mobi prt. E  ounce price sqlite s	zast  e tra  ille/C  3aza  w pr  TER  TER  ANALL  2  2  2  2  2  2  2  2  2  2  2  2	ZRSS   Filt   Silt	sqlite ainers jest s: adku v oczna  I ziimestam filte filt filt filt filt filt filt filt filt	zna zna zyfr wer i jes  P EXEMPLE	ANGLE Phone X MORLE MORLE Phone X MORLE Phon	SIĘ W ICO DICATIC  DE SIĘ W ICO DICATIC  A. Tablic  droid. P  SIŻEJ:  SM-G920F  Redmi Note 8 Pro  MARI  ARRI MARI  Redmi Note 8 Pro  MARI  SM-G920F  Redmi Note 8 Pro  MARI  MARI  Redmi Note 8 Pro  MARI  SM-G920F  Redmi Note 8 Pro  MARI  Redmi Note 8 Pro  RAGRI  SM-G920F  Redmi Note 8 Pro  RAGRI  SM-G920F  Redmi Note 8 Pro  MARI  REDMI NOTE 8 Pro  RAGRI  RAGRI  REDMI NOTE 8 Pro  RAGRI  REDMI NO	PRGGShujhLZEW Scanning started frap/Gaskjiarurw PRGGShujhLZEW Scanning started frap/Gaskjiarurw PRGGShujhLZEW Scanning started frap/Gaskjiarurw Frap/Gaskjiarurw Frap/Gaskjiarurw Frap/Gaskjiarurw Frap/Gaskjiarurw Scanning started PRGGShujhLZEW Scanning started PRGGShujhLZEW Scanning started frap/Gaskjiarurw Scanning started scanning started prGGSShujhLZEW Scanning started scanning started scanning started scanning started scanning started	JI  -UUID/Library COUNTER zaw Owa zawartoś  ZMSG  ZMSG  ZMSG  IDOyWIJOXIIZIIm64u/s1YF2VC/ysGdZIX Chk1joPBMAXFZUmt65zArpvWBdCQs: CDOyWIJOXIIZIIm64u/s1YF2VC/ysGdZIX Chk1joPBMAXFZUmt65zArpvWBdCQs: Chk1joPBMAXFZUmt6QscArp	New Rec  P92FXB2Qcc13ELPPdegwtrO.  64Zm+/3MC12wRpZ0/1394k.  192FXB2Qcc13ELPPdegwtrO.  194Zm+/3MC12wRpZ0/1394k.  194Zm+/3MC12wRpZ0/1394k.  194Zm+/3MC12wRpZ0/1394k.  194Zm+/3MC12wRpZ0/1394k.  194Zm+/3MC12wRpZ0/1394k.  194Zm+/3MC12wRpZ0/1394k.  194Zm+/3MC12wRpZ0/1394k.  194Zm+/3MC12wRpZ0/1394k.  194Zm+/3MC12wRpZ0/1394k.	DINE  JORG  JORG  Filter  AUMAL  MULL  MUL
	Zal  Bai /va  Sul wp  ZEI  Table:  1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26	Za:  Zar/I  ppo  isy  NC  ZENC Z PK Z  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	amy sqlite mobi prt. E  ounce price sqlite s	zast  tra ile/C  3aza  w pr  TER  TER  TER  AMAL  2  AMAL  2  AMAL  2  AMAL  2  AMAL  4  AMAL  2  AMAL  4  AMAL  2  AMAL  4  AMAL  AMAL	ZRSS wid  ZRS wid  ZRSS wi	sqlite ainers jest si adku v Oczna  1 ZTIMESTAM Filter 610444231. 610444231. 610444291. 610444291. 610444291. 610444350. 610444350. 610444350. 610444415. 610444415. 610444415. 610444415.	zna s/Da zyfr wer i jes  rixpow i 100 i 400 i 400 i 400 i 100 i 400 i 40	A STATE STATE OF THE STATE OF T	SIĘ W ICO  OPPLICATION  A. Tablic  droid. P  Liżej:  ZMODELP  Filter  NURL  SM-0920F  Redmi Note 8 Pro  NARL  SM-0920F  Redmi Note 8 Pro  SM-0920F  NARL  ARRIL  Redmi Note 8 Pro  SM-0920F  NARL  NAR	PROGRAIJE Stanning started frag/foskylarusw Scanning started PROGRAIJE Stanning started PROGRAIJE Stanning started PROGRAIJE Scanning started frag/foskylarusw Scanning stopped Scanning started frag/foskylarusw Scanning started frag/foskylarusw Scanning started PROGRAIJE Scanning started Scanning started Scanning started Scanning started Scanning started V2pTisb/S2D[Xcau	JI  -UUID/Library  COUNTER zaw  Owa zawartoś  ZM5G  ZM5G  ZM5G  ZM5G  ZM5G  ID0yWijoxttzflim64u/s1YF2VCysGdZIX  chk.ljoParMAXFZUmt65zArpvWll8dCqs:  chk.ljoParMAXFZUmt65zArpvWll8dCqs:  (chk.ljoParMAXFZUmt65zArpvWll8dCqs:  Librywijoxttzflim64u/s1YF2VCysGdZIX  chk.ljoParMAXFZUmt65zArpvWll8dCqs:  Librywijoxttzflim64u/s1YF2VCysGdZIX  chk.ljoParMAXFZUmt65zArpvWll8dCqs:  Librywijoxttzflim64u/s1YF2VCysGdZIX  chk.ljoParMAXFZUmt65zArpvWll8dCqs:  Librywijoxttzflim64u/s1YF2VCysGdZIX  chk.ljoParMAXFZUmt65zArpvWll8dCqs:  Chk.ljoParMAXFZUmt65zArpvWll8dCqs:  Chk.ljoParMAXFZUmt65zArpvWll8dCqs:  Chk.ljoParMAXFZUmt65zArpvWll8dCqs:  Chk.ljoParMAXFZUmt65zArpvWll8dCqs:	New Rec	DINE  JORG  JORG  Filter  AUMAL  MULL  MUL



#### 6.9. SEQ20200500309

PODATNOŚĆ	[Android] Brak zaimlementowanego mechanizmu certificate-pinnning	PRIORYTET	ŚREDNI				
CVSS VECTOR	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	CVSS:3.0 base score	5.9				
OPIS	Aplikacja nie implementuje zwiększającego bezpieczeństwa mechanizmu certificate pinning. Brak zaimplementowanego mechanizmu może prowadzić do ataków MITM w przypadku zainfekowania zrootwanego urządzenia złośliwym oprogramowaniem.						
ZALECENIA	Stworzyć plik konfiguracyjny networ_securtiy_ kluczy publicznych wykorzystywanych do realiz						
SZCZEGÓŁY TECHNICZNE	Połączenia pomiędzy aplikacjami ProtegoSafe a https://safesafe.app ładowanym w komponency widoczną dla użytkownika logikę aplikacji) są za protokołu HTTPS. Aplikacje nie implementują je bezpieczeństwa mechanizmu certificate pinnin może prowadzić do ataków MITM w przypadku lub jailbreakowanego urządzenia złośliwym opwykorzystania podatności dostępny jest w opis SEQ20200500310.	cie WebView (; abezpieczone p ednak zwiększa g. Brak certific u zainfekowani rogramowanie	orzy użyciu ającego ate pinningu a zrootwanego				



#### 6.10. SEQ20200500310

PODATNOŚĆ	[iOS] Brak zaimlementowanego mechanizmu certificate-pinnning	PRIORYTET	ŚREDNI
CVSS VECTOR	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	CVSS:3.0 base score	5.9
OPIS	Aplikacja nie implementuje zwiększającego bez certificate pinning. Brak zaimplementowanego do ataków MITM w przypadku zainfekowania z złośliwym oprogramowaniem.	mechanizmu	może prowadzić
ZALECENIA	W przypadku wykorzystania biblioteki Alamofii ServerTrustManager. W przypadku NSURLSessi URLSession:didReceiveChallenge:completionHa	ion, wykorzyst	ać
SZCZEGÓŁY TECHNICZNE	Połączenia pomiędzy aplikacjami ProtegoSafe a https://safesafe.app ładowanym w komponency widoczną dla użytkownika logikę aplikacji) są za protokołu HTTPS. Aplikacje nie implementują je bezpieczeństwa mechanizmu certificate pinnin może prowadzić do ataków MITM w przypadku lub jailbreakowanego urządzenia złośliwym operzykład wykorzystania podatności jest widocz stanu zdrowia została podmieniona:	cie WebView ( abezpieczone p ednak zwiększa g. Brak certific u zainfekowani rogramowanie	orzy użyciu ającego ate pinningu a zrootwanego m.
	Aaaa, przeanalizowaliśmy Twoje odpowiedzi. Wynik testu z 10-05-2020 kwalifikuje Cię do grupy:  Wykonaj TEST oceny ryz  To jest złośliwa treść wyniku zdrowia Szczególnie niepokoj objawy:	oceny	



#### 6.11. SEQ20200500311

PODATNOŚĆ	[Android / iOS] Aplikacje pozwalają na wykonywanie backupów	PRIORYTET	WYSOKI			
CVSS VECTOR	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	CVSS:3.0 base score	7.5			
OPIS	Aplikacja ProtegoSafe umożliwia wykonywanie kopii zapasowych. Kopie zapasowe aplikacji umieszczane są automatycznie w chmurze (GoogleDrive lub iCloud), mogą też być wykonane lokalnie. Ponieważ pliki aplikacji zawierają nieszyfrowane dane medyczne (ankiety dotyczące stanu zdrowia), może to prowadzić do ich wycieku w przypadku przejęcia konta użytkownika przez atakującego (backup w chmurze) lub kradzieży telefonu.					
ZALECENIA	Zalecamy wyłączyć możliwość tworzenia kopii z Android w pliku AndroidManifest.xml poprzez false (android:allowBackup="false") lub stworz z niego local storage. Dla aplikacji iOS poprzez isExcludedFromBackup() wyłączyć możliwość b zawierających wrażliwe dane.	zmianę flagi <i>al</i> yć reguły back wykorzystanie	lowBackup na upu wyłączające API			
SZCZEGÓŁY TECHNICZNE	N/D					



#### 6.12. SEQ20200500312

PODATNOŚĆ	[Android] Ograniczenia dotyczące czasu przechowywania i usuwania tymczasowych identyfikatorów mogą zostać ominięte poprzez modyfikację czasu systemowego	PRIORYTET	ŚREDNI
CVSS VECTOR	AV:P/AC:L/PR:L/UI:R/S:C/C:N/I:H/A:N	CVSS:3.0 base score	4.9
OPIS	Aplikacje dla systemów Android oraz iOS wyko referencyjny do określenia czasu ważności zapi tymczasowych. Zegar systemowy może być do użytkownika lub zmodyfikowany bez wiedzy uż mechanizm NITZ - uzyskiwania nazwy usługoda aktualnej strefy czasowej. Modyfikacje czasu sy w omawianym przypadku na usunięcie wszystkidentyfikatorów zapisanych w bazie lub wstrzy identyfikatorów.	sanych identyf wolnie modyfil cytkownika np. iwcy GSM oraz cystemowego po tich rekordów	fikatorów kowany przez poprzez daty i godziny ozwalają tymczasowych
ZALECENIA	Zalecamy porzucić wykorzystanie czasu system czasu poprzez protokół NTP, Network Time Prozostać zaimplementowany w aplikacji ProteGo zmiany czasu operacje powinny wykorzystywać czasu.	otocol. Klient N Safe, a wszyst	TP powinien kie wrażliwe na
SZCZEGÓŁY TECHNICZNE	N/D		



#### 6.13. SEQ20200500313

PODATNOŚĆ	[iOS] Tymczasowe identyfikatory napotkanych urządzeń nie są usuwane z bazy danych aplikacji	PRIORYTET	INFO
CVSS VECTOR	N/D	CVSS:3.0 base score	N/D
OPIS	Tymczasowe identyfikatory zapisane w bazie d trzy tygodnie nie są usuwane.	anych tracer.so	qlite starsze niż
ZALECENIA	Dodać logikę usuwającą przestarzałe identyfika NTP jako źródło czasu.	itory wykorzys	tując protokół
SZCZEGÓŁY TECHNICZNE	N/D		

#### 6.14. SEQ20200500314

PODATNOŚĆ	[Android / iOS] Możliwość przeprowadzenia ataków typu relay attack	PRIORYTET	ŚREDNI	
CVSS VECTOR	AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:L	CVSS:3.0 base score	5.4	
OPIS	atakami relay attack. Wiadomość lub wiadomo pozyskane przez atakującego w jednej lokalizac i rozgłoszone w innej. W szczególnej sytuacji m wiadomości Encounter Message z lokalizacji o potencjalnych zakażeń (poradnia, izba przyjęć, retransmisja wiadomości do strategicznej lokal	Wykorzystana biblioteka OpenTrace nie zapewnia skutecznej ochrony przed atakami relay attack. Wiadomość lub wiadomości Encounter Message pozyskane przez atakującego w jednej lokalizacji mogą zostać przesłane i rozgłoszone w innej. W szczególnej sytuacji możliwe jest pozyskanie wiadomości Encounter Message z lokalizacji o dużym prawdopodobieństwie potencjalnych zakażeń (poradnia, izba przyjęć, szpital), i równoczesna retransmisja wiadomości do strategicznej lokalizacji (urząd gminy, miasta, sejm, senat). Wynikiem działania może być objęcie kwarantanną osób, które nie posiadały kontaktu z zarażonymi osobami.		
ZALECENIA	Brak dla wykorzystanej biblioteki. Zalecamy wykorzystanie protokołu DP3T, który minimalizuje możliwość przeprowadzenia skutecznego ataku relay attack.			
SZCZEGÓŁY	Określono brak odporności biblioteki OpenTrace na ataki typu replay i relay attack. Ze względu na przyjęty model działania bilbioteki OpenTrace			



#### **TECHNICZNE**

wykorzystujący Bluetooth Advertising oraz zakładając zmienność tymczasowych identyfikatorów co 15 minut, możliwe jest przeprowadzenie ataków replay i relay attack, gdzie potencjalny atakujący wykorzystując uprzednio przygotowane oprogramowanie, będzie w stanie pozyskać pakiety rozgłaszane z ProteGoSafe zawierające tymczasowy identyfikator wraz z modelem telefonu oraz identyfikatorem organizacji i w takiej samej formie powielać (retransmitować) pozyskane wiadomości w swoim otoczeniu. Przykładowa format i zawartość wiadomości Encounter Message rozgłaszanej przez ProteGo Safe widoczna jest poniżej.

```
"uuid": "6e9e7830f4c74717b0d8525d30181121",
   "characteristics":
     {
       "uuid": "8fbfdf095eb44f68ac166cd2275d07ca",
       "value":
"7b226964223a222f74303856316c37723058344e6932696f5330582b67
697548666379596b2b6438627742374668717a59362f776b7a68517632
62534e68596d6176307948762b487952627631755a503478373632626
b73673d3d222c226d70223a225265646d69204e6f746520382050726f2
22c226f223a22504c5f504753222c2276223a327d",
       "asciiValue":
"{\"id\":\"/t08V1I7r0X4Ni2ioS0X+giuHfcyYk+d8bwB7FhqzY6/wkzhQv
2bSNhYmav0yHv+HyRbv1uZP4x762bksg==\",
      \"mp\":\"Redmi Note 8 Pro\",
      \"o\":\"PL_PGS\",
                                               \"v\":2}"
     }
```

Możliwe jest również przesłanie pozyskanej wiadomości do zupełnie innej fizycznej lokalizacji oraz jej retransmisja poprzez Bluetooth aż do wygaśnięcia czasu jej ważności. Powielenie takiego scenariusza na dużą skalę pozwoli potencjalnemu atakującemu całkowicie zaburzyć wynik działania algorytmu dopasowującego działającego na backendzie. Należy również wziąć pod uwagę scenariusz, gdzie atakujący w dłuższym okresie czasu pozyskuje wiadomości Encounter Message z lokalizacji o dużym prawdopodobieństwie zakażeń (poradnia, izba przyjęć, szpital), i równocześnie retransmituje wiadomości do strategicznej lokalizacji (urząd gminy, miasta, sejm, senat). Wynikiem działania może być objęcie kwarantanną osób, które nie posiadały kontaktu z zarażonymi osobami.



#### 6.15. SEQ20200600201

PODATNOŚĆ	[Backend] Możliwość enumeracji poprawnych kodów PIN dla endpointa /getAccessToken	PRIORYTET	KRYTYCZNY	
CVSS VECTOR	AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:H	CVSS:3.0 base score	9.9	
OPIS	Zwracanie statusu 404 oraz statusu "Invalid code" w przypadku błędnego kodu PIN pozwala atakującemu na enumerację poprawnych kodów PIN oraz pozyskanie poprawnego tokenu JWT pozwalającego na upload danych wykorzystaniem /uploadDiagnosisKeys. Scenariusz może zostać zrealizowany w oknie czasowym pomiędzy wygenerowaniem kodu PIN poprzez operatora w Centrum Kontaktów, a finalnym wykorzystaniem go w aplikacji przez użytkownika. Możliwość wykorzystania podatności jest powiązana bezpośrednio z SEQ20200600202.			
ZALECENIA	Logika aplikacji nie powinna ujawniać poprawności kodu PIN. Zalecamy dla requestów zawierających niepoprawny kod PIN również zwracać poprawną odpowiedź z tokenem JWT. Token powinien zostać zwalidowany w następnym kroku, czyli uploadowaniu danych z wykorzystaniem endpointu /uploadDiagnosisKeys. Wtedy powinna zostać zwalidowana poprawność tokena i PIN oraz podjęta decyzja czy uploadowane dane powinny zostać odrzucone czy przyjęte do dalszej analizy.			
SZCZEGÓŁY TECHNICZNE	zwraca tokan IMT w nolu <i>gccessToken</i> jak na przykładzie przedstawionym			
	{"result":{"accessToken":"eyJhbGciOiJIUzUxMilsInR5cCl6lkpXVCJ9.eyJjb2RlljoiTUJZODAwliwiaWF 0ljoxNTkxMTg3Njc1LCJleHAiOjE1OTExODk0NzUsImp0aSl6lmlxZGQ3NGViLWVlODgtNDU0OS04Y WQ0LTQ1MWZkODRhNDJkZCJ9.ejjcwnaz2PtWWFAya9zCEzLuR_2yl9KTLZlZY-vellYJ3PbztcN9- CRgQx7gim3ra9XcKfNbxks8RNKXlvROvw"}}			
	W przypadku przekazania niepoprawnego kodu PIN endpoint /getAccessToken zwraca błąd jak na przykładzie poniżej:			
	{"error":{"message":"Invalid code","status":"NOT_FOUND"}}			



#### 6.16. SEQ20200600202

PODATNOŚĆ	[Backend] Brak lin /getAccessToken	nitu żądań dla s	erwisu	PRIORYTET	WYSOKI	
CVSS VECTOR	AV:N/AC:L/PR:N/U	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H			7.5	
OPIS	W wyniki takiej ko skutecznego ataku	Endpoint /getAccessToken nie posiada zabezpieczeń typu rate-limiting.  W wyniki takiej konfiguracji serwisu możliwe jest przeprowadzenie skutecznego ataku brute force którego celem jest 'odgadywanie' kodu PIN w celu pozyskania tokenu JWT umożliwiającego upload danych.				
ZALECENIA	Wprowadzić mech	anizm rate-limi	ting dla end	pointu / getAc	cessToken.	
SZCZEGÓŁY TECHNICZNE	zapytania pochodziły z jednego komputera (jeden adres IP). Poniżej przedstawiony jest dowód w postaci żądania i odpowiedzi z serwera wraz z uzyskanym w ten sposób tokenem JWT.					
		Payloads Options			?	
	Filter: Showing all Items   Request   Payload   340478   YYQ700   393159   2WX800   393995   QDE800   416493   8WL800   416493   8WL800   452034   DUB900   271555   QRJ500   271565   ERJ500   271568   RRJ500   271566   DRJ500   271566   DRJ500   271566   DRJ500   271566   DRJ500   271566   DRJ500   271566   DRJ500   DRJ500	Status   Error	Timeout   Length   880	Contair Contair Contair Contair Contair		
	Request Response  Raw Headers Hex JSON	Web Tokens				
	1 HTTP/1.1 200 OK 2 Content-Type: applicat 3 Etag: W'N19-DeHtCBdqhE 5 Vary: Origin 6 X-Powered-By: Express 7 X-Cloud-Trace-Context: 8 Date: Wed, 03 Jun 2020 9 Server: Google Fronten 10 Content-Length: 281 11 Alt-Svc: h3-27=":443"; ma-2592000,h3-0050=":4 2 connection: close 12 ("result": ("accessTote 4 ("result": ("accessTote 4 "yJhbGc101IUzUxHisi	ion/json; charset=ut UGZY4fKTbhUaKcXp7o" 7hhp5oc68931 d66ad2477770f756f8d 12:34:35 GMT d ma=2592000,h3-25=": 43"; ma=2592000,h3-Q 43"; ma=2592000,h3-Q nBscc161kpXVCJ9.eyJj	357d77d07760a 143"; ma=2592000 149=":443"; ma=2 143=":443"; ma=2	592000, h3-Q048=":443 592000, quic=":443";	ma=2592000; v="46,43" ma=2592000; v="46,43" SNjclLCJleHAiOjElOTExO PtWFAyaSzCEzLuR 2y19K  0 matches Pretty	



#### 6.17. SEQ20200600203

PODATNOŚĆ	[Backend] Brak limitu żądań dla serwisu /generateCode	PRIORYTET	WYSOKI
CVSS VECTOR	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	CVSS:3.0 base score	7.5
OPIS	Endpoint /generateCode nie posiada zabezpieczeń typu rate-limiting.  W wyniku takiej konfiguracji serwisu możliwe jest przeprowadzenie skutecznego ataku brute force dzięki czemu istnieje możliwość wygenerowania dowolnej ilości nowych kodów PIN. Ten atak w szczególnym przypadku może doprowadzić do odmowy obsługi żądania (DoS) lub innego nieprzewidywalnego zachowania w momencie kiedy wyczerpany zostanie zakres znaków możliwy w kodzie PIN [A-Z,0-9].		
ZALECENIA	Wprowadzić mechanizm rate-limiting dla endpointu /generateCode.		
SZCZEGÓŁY TECHNICZNE	N/D		



#### 6.18. SEQ20200600204

PODATNOŚĆ	[iOS] Możliwość obejścia mechanizmu ograniczenia ilości prób wpisania kodu PIN	PRIORYTET	WYSOKI	
CVSS VECTOR	AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:L	CVSS:3.0 base score	7.2	
OPIS	Użytkownik ma możliwość podania kodu PIN, który uprzednio pozyskał z Centrum Kontaktów, w celu uploadu swoich kluczy. Aplikacja ogranicza ilości nieudanych prób wpisania kodu PIN, z każdą powiększającą się nieudaną ilością prób przedłużając okres, po jakim wprowadzone mogą zostać nowe kody PIN (5 min, 1 godzina, 1 doba).			
	Walidacja okresu czasu, po jakim użytkownik może wykonać ponowne prowpisania kod PIN, bazuje na czasie systemowym urządzenia, który może zostać dowolnie zmodyfikowany przez użytkownika.  Dokonując więc modyfikacji czasu systemowego użytkownik jest w stanie obejść ograniczenia czasowe, tym samym ilości prób wpisania kodu PIN w celu brute-forcowania kodu PIN.			
	Zauważono również, że licznik ilości prób nie jest zaimplementowany poprawnie co widać na załączonym zrzucie ekranu w kolejnej sekcji.			
ZALECENIA	Do obliczenia różnicy czasu, po jakim użytkownik może ponownie wpisać kod PIN, zalecamy wykorzystanie protokołu synchronizacji czasu NTP zgodnie z normą RFC5905. W szczególnym przypadku, kiedy synchronizacja czasu z serwerem NTP nie może się odbyć z powodów innych niż brak dostępu do sieci, fallback do czasu systemowego.			
SZCZEGÓŁY TECHNICZNE	00:46I ≎			
	Wprowadź kod PIN otrzymany od Operatora Centrum Kontaktu. Dzięki temu dasz innym znać, że mogli mieć kontakt z koronawirusem. Nie martw się, informacje są w pełni anonimowe.  J D D N J D  Twój PIN jest niepoprawny lub wygasł. Sprawdź poprawność kodu PIN i spróbuj ponownie. (Próba 135 z 60)			



#### 6.19. SEQ20200600205

PODATNOŚĆ	[Android] Możliwość obejścia mechanizmu ograniczenia ilości prób wpisania kodu PIN	PRIORYTET	WYSOKI	
CVSS VECTOR	AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:L	CVSS:3.0 base score	7.2	
OPIS	Użytkownik ma możliwość podania kodu PIN, który uprzednio pozyskał z Centrum Kontaktów, w celu uploadu swoich kluczy. Aplikacja ogranicza ilość nieudanych prób wpisania kodu PIN, z każdą powiększającą się nieudaną ilością prób przedłużając okres, po jakim wprowadzone mogą zostać nowe kody PIN (5 min, 1 godzina, 1 doba).			
	Walidacja okresu czasu, po jakim użytkownik może wykonać ponowne próby wpisania kod PIN, bazuje na czasie systemowym urządzenia, który może zostać dowolnie zmodyfikowany przez użytkownika.  Dokonując więc modyfikacji czasu systemowego użytkownik jest w stanie obejść ograniczenia czasowe, tym samym ilości prób wpisania kodu PIN w celu brute-forcowania kodu PIN.  Zauważono również, że licznik ilości prób nie jest zaimplementowany poprawnie co widać na załączonym zrzucie ekranu w kolejnej sekcji.			
ZALECENIA	Do obliczenia różnicy czasu, po jakim użytkownik może ponownie wpisać kod PIN, zalecamy wykorzystanie protokołu synchronizacji czasu NTP zgodnie z normą RFC5905. W szczególnym przypadku, kiedy synchronizacja czasu z serwerem NTP nie może się odbyć z powodów innych niż brak dostępu do sieci, fallback do czasu systemowego.			
SZCZEGÓŁY TECHNICZNE	14:21 Æ \$ .⊪			
	Wprowadź kod PIN otrzymany od Operatora Centrum Kontaktu. Dzięki temu dasz innym znać, że mogli mieć kontakt z koronawirusem. Nie martw się, informacje są w pełni anonimowe.  D D K D  Twój PIN jest niepoprawny lub wygasł. Sprawdź poprawność kodu PIN i spróbuj ponownie. (Próba 65 z 60)			



#### 6.20. SEQ20200600206

PODATNOŚĆ	[Backend] Brak nagłówków http odpowiedzialnych za bezpieczeństwo (Strict- Transport-Security, X-Frame-Options, X-XSS- Protection), brak mechanizmu Content Security Policy	PRIORYTET	ŚREDNI	
CVSS VECTOR	AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P	CVSS:3.0 base score	5.4	
OPIS	Brak nagłówka "Strict-Transport-Security" Może w różnych sytuacjach powodować powstawanie bardziej poważnych podatności takich jak XSS czy MITM. Brak tego nagłówka może poprawić skuteczność ataku sslstrip i w konsekwencji do np. przejęcia sesji użytkownika lub innych wrażliwych danych.  Nagłówek X-Frame-Options: SAMEORIGIN nie jest obecny we wszystkich odpowiedziach serwera. Nagłówek X-Frame-Options określa czy możliwe jest ładowanie strony w ramce. Wdrożenie tego nagłówka zapewnia dla strony zwiększenie ochrony przeciw atakom typu Clickjacking uniemożliwiając ich wczytywanie przez inne niezaufane strony.  Dobrą praktyką ochrony przed XSS jest prewencyjny mechanizm anty-XSS który zaimplementowany jest w przeglądarkach. Przeglądarka weryfikuje czy kod js który ma zostać wykonany na stronie (znajduje się w odpowiedzi serwera) nie znajduje się również w żądaniu które do serwera dotarło.  Content Security Policy (CSP) obsługiwany przez współczesne przeglądarki, stanowi skuteczne narzędzie prewencyjne przeciw atakom XSS.  Implementacja odpowiednich dyrektyw daje przeglądarce instrukcje, które elementy mają być załadowane a które nie w zależności od ich źródła.  Poprawna konfiguracja zablokuje wszelkie próby dołączenia skryptów js pochodzących z innych miejsc niż te określone w polityce. Polityka CSP wymaga szczegółowej analizy systemów oraz dołączanych zasobów przed wdrożeniem tego mechanizmu. Zaleca się również gruntowne testy tego rozwiązania. Poniżej przykładowe rozwiązanie: Content-Security-Policy: default-src 'self' https://domenax.pl https://*.domenax.pl co pozwala na załadowanie zewnętrznych zasobów tylko jeśli pochodzą z domeny domenax.pl lub dowolnej subdomeny domenax.pl.			
ZALECENIA	Nagłówek ustawiony dla wszystkich odpowiedzi z serwera z godnie z poniższym:			
Strict-Transport-Security: max-age:31536000; includeSubDomains; preload X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block				



#### SZCZEGÓŁY **TECHNICZNE**

#### Dotyczy:

https://europe-west3-safesafe-test.cloudfunctions.net/generateCode https://europe-west3-safesafe-test.cloudfunctions.net/getAccessToken

#### Request:

```
POST /generateCode HTTP/1.1
Host: europe-west3-safesafe-test.cloudfunctions.net
Content-Type: application/json;charset=utf-8
api-token: dW6jcHnsG2TS7pKmqrVq3mNGA8Vt9Tp7G3aQYKKE\\
Content-Length: 20
"data" : null
```

#### Odpowiedź:

```
HTTP/1.1 200 OK
               Content-Type: application/json; charset=utf-8
               Etag: W/"13-oeLEdka2vWI9yVxbTN4fBQZppi0"
               Function-Execution-Id: lhjhse551jz6
               Vary: Origin
               X-Powered-By: Express
               X-Cloud-Trace-Context: b3b5b042c2e3d8b4408d70b48cf3be06;o=1
               Date: Wed, 03 Jun 2020 11:21:59 GMT
               Server: Google Frontend
               Content-Length: 19
               Alt-Svc: h3-27=":443"; ma=2592000,h3-25=":443"; ma=2592000,h3-T050=":443";
ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q049=":443"; ma=2592000,h3-Q048=":443";
ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443";
ma=2592000; v="46,43"
               {"result":"9H7JV1"}
```

## SEQRED

SEQRED S.A. ul. Rybnicka 52 02-432 Warszawa tel.: +48 22 292 32 23 fax: +48 22 292 32 21 biuro@seqred.pl www.seqred.pl

Znajdź nas na:







