

SEQRED

Raport podsumowujący testy bezpieczeństwa

Produkt: ProteGo Safe

Klient: Ministerstwo Cyfryzacji

05.08.2020

www.seqred.pl

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.	PODSUMOWANIE ZARZĄDCZE	3
2.	Aktualny status podatności	6
3.	Etap I – 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 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	18
6.5.	SEQ20200500305	19
6.6.	SEQ20200500306	20
6.7.	SEQ20200500307	21
6.8.	SEQ20200500308	22
6.9.	SEQ20200500309	23
6.10.	SEQ20200500310	24
6.11.	SEQ20200500311	25
6.12.	SEQ20200500312	26
6.13.	SEQ20200500313	27
6.14.	SEQ20200500314	27
6.15.	SEQ20200600201	29
6.16.	SEQ20200600202	30
6.17.	SEQ20200600203	31
6.18.	SEQ20200600204	32
6.19.	SEQ20200600205	33
6.20.	SEQ20200600206	34

1. PODSUMOWANIE ZARZĄDCZE

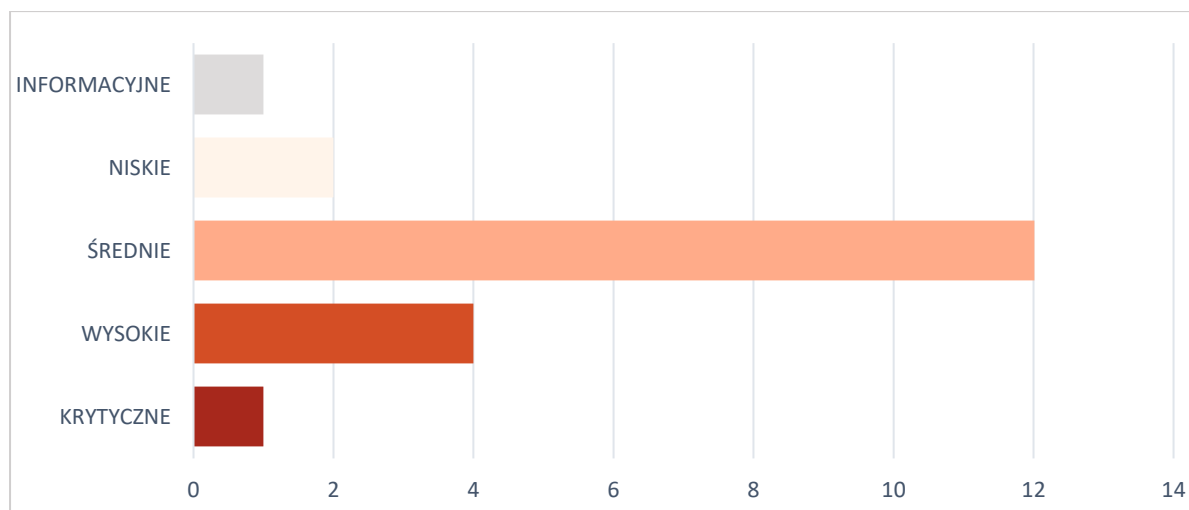
Poniższy dokument stanowi podsumowanie prac zleconych przez Ministerstwo Cyfryzacji firmie SEQRED S.A. w zakresie oceny bezpieczeństwa rozwiązania ProteGo Safe.

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 przetamania 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 różnych 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	[Android] 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	Naprawione
SEQ20200500312	ŚREDNI	Błąd logiczny	[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
SEQ20200600203	WYSOKI	Brak mechanizmu rate-limiting	[Backend] Brak limitu żądań dla serwisu /generateCode	Naprawione
SEQ20200600204	WYSOKI	Ominięcie wbudowanych mechanizmów zabezpieczających	[iOS] Możliwość obejścia mechanizmu ograniczenia ilości prób wpisania kodu PIN	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

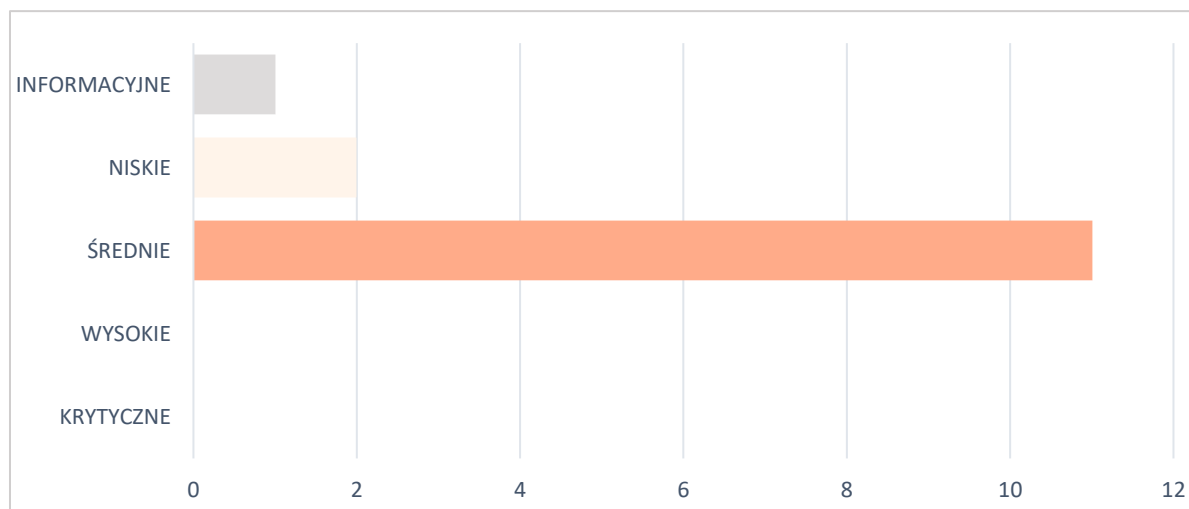
Lokalizacja testów	Warszawa
Data rozpoczęcia	04.05.2020
Data zakończenia	15.05.2020
Nazwa aplikacji, Android	ProteGO Safe
Wersja aplikacji, Android	3.0.3
Nazwa pakietu, Android	pl.gov.mc.protegosafe
Sumy kontrolne, Android	MD5:c70fa1e8edbe06e9fa1d29ddd540518c SHA1:fec8c5859c1e24943aeadeafc9d0c1482ad90254 SHA256:03e116b831b184842ea96bb17f7880439addf5cb724da54c735b730f34eb44dc
Nazwa aplikacji, iOS	ProteGO Safe
Wersja aplikacji, iOS	3.0.2
Identyfikator, iOS	pl.gov.mc.protegosafe
Sumy kontrolne, iOS	MD5:9074acc39c6ab0c063caaec769ecc848 SHA1:188fb3dd1d7bfebc73ab5dda4292df7c4da7e2e2 SHA256:2edd10c6da64c3d9b638f19c91d3d7337259f36b3fc50f4016aca5dfd6e65e90

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	[iOS] Aplikacja nie posiada wbudowanego mechanizmu jailbreak detection
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.

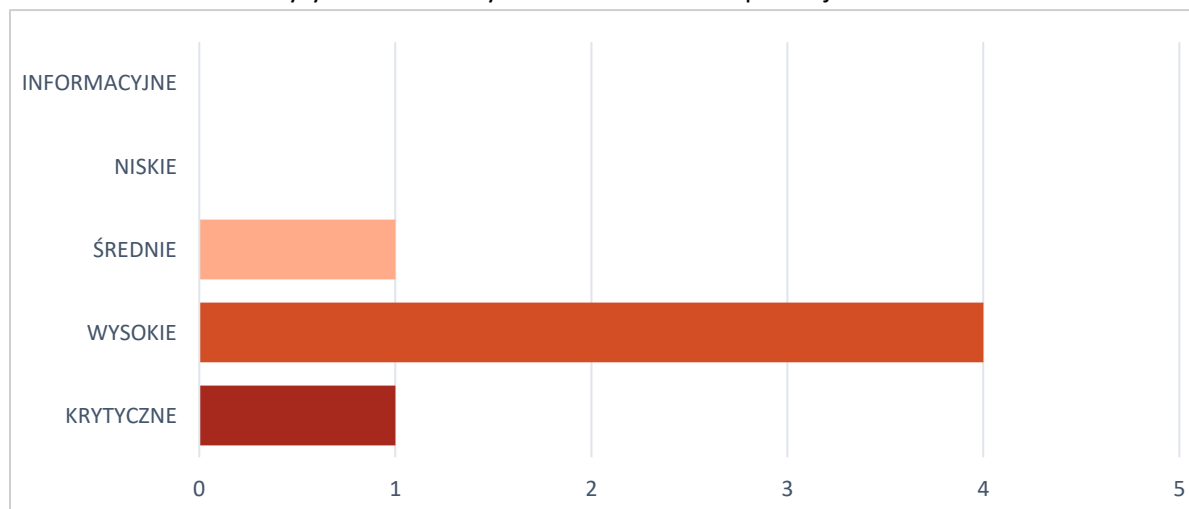
W toku uzgodnień potwierdzono wyłączenie z zakresu testów komponentu Centrum Kontaktów.

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 <https://github.com/ProteGO-Safe>. W testowanych wersjach aplikacji mobilnych biblioteka OpenTrace została zastąpiona poprzez wykorzystanie API Exposure Notification

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

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: d09c7eaeedb4328fa2a837f3ef57be292798731

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 przez 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 siecią 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. Czyny 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 oraz refreshedToken <pre>D/zzy (5648): FCM_token cNYg08qjSxukhYf1neJHb_:APA91bFp9ovVnBR0byQ8DSuVFm1pWzNzwHa2ms4YqLYR8I8SIyQSnDLWbJwKTRnoqfslst_wHw1VLFLZASXFgaJb4kKsuYnIR0C7-1 D/FirebaseMessagingService(5648): Refreshed token: cNYg08qjSxukhYf1neJHb_:APA91bFp9ovVnBR0byQ8DSuVFm1pWzNzwHa2ms4YqLYR8I8SIyQSnDLWbJwKTRnoqfslst_wHw1VLFLZASXFgaJb4kKsuYnIR0C7-1</pre>		

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 zrootowanych urządzeniach. Użytkownicy posiadający zrootowane urządzenia są bezpośrednio podatni na kradzież wrażliwych danych opisanych w SEQ20200500304, SEQ20200500305 oraz SEQ20200500306.		
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 jailbreakowanych urządzeniach. Użytkownicy posiadający takie urządzenia są bezpośrednio podatni na kradzież wrażliwych danych opisanych w SEQ20200500306, SEQ20200500307 oraz SEQ20200500308.		
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 formie niezaszyfrowanej w pliku /data/data/pl.gov.mc.protegosafe/files/tempIDs. Atakujący, który uzyska dostęp do systemu plików na urządzeniu może pozyskać identyfikatory, które użytkownik rozgłasza I będzie rozgłaszał w najbliższym czasie.		
ZALECENIA	Zalecamy wprowadzenie mechanizmu root-detection, który ograniczy problem dostępu do wrażliwych danych na zrootowanych urządzeniach. Zalecamy przechowywać tymczasowe identyfikatory w szyfrowanej formie.		
SZCZEGÓŁY TECHNICZNE	<pre> /data/data/pl.gov.mc.protegosafe/files # cat tempIDs [{"expiryTime":1589114571,"tempID":"btd3HYF7B3V4s8ljwtt4gjGP81AWal01bs+EK9dzclmQZot/TyYP URtZTbYLLtzK5xdZBoAvfc48xdIWnQ==","startTime":1589113671},{"expiryTime":1589115471,"tempID ":"upRs+G2Jbj1Yi+/A7wfwXmSGVCMXSc76iz1DBM+O3usmhsoBqG2kdf01vwZP+I+p3AFzq4EZZ4ppMy 2YQ==","sta rtTime":1589114571},{"expiryTime":1589116371,"tempID":"5c4BbVgZtaMztz+XBD7drIROtXD3fKof9Jb prm6csNWX38f+IKksW9tj78zAJoorwAV8tu75WgKu+NftA==","startTime":1589115471},{"expiryTime" :1589117271,"tempID":"lr2fe6tu9Mp94KBC3c7gOPjbEvFiRYRL6Wnzwyewg29SRAUHTGCub9TH8rPDzd DolQ6DtJf 9J+J1vShM0Q==","startTime":1589116371},{"expiryTime":1589118171,"tempID":"v3e70V5kXyyTmMS ievE72biGQDDQXc9pFSArmpBH0W5W0zOZFu6rPbORbwKSMxzRfQ5O1w4rTnyRHVvO6Q==","startTi me":1589117271},{"expiryTime":1589119071,"tempID":"su5PCcQhIYQk86DdlHQ2UvBqjjKoAKVDdf4X DDoujyx8lVrqe2m+ 3f2ifjxmjeH7eCi4GmM1YbfbD2AVcw==","startTime":1589118171},{"expiryTime":1589119971,"templ D":"AJUSsi2cYtgnxXR3CiLu1bQyCDkrXSHh+kDEE1P/L7QMrmUWOZfPpN44lhqb+0ImRUTKSdAd5tZpTgl hsw==","startTime":1589119071},{"expiryTime":1589120871,"tempID":"dW6lpg2ulLcCEZQg2SLmCces a2jBITar6 p/hoywnY237DEye55d1PR3f/vi0GGEX46oE3NEs91JJT13EiQ==","startTime":1589119971},{"expiryTime ":1589121771,"tempID":"6JmFKhG46iAnXJ4a/L/9OVnl9aiwVq/6D2SwCgtlml1aP+PiVhCk9JZBQFzV1yW 3OYoXzI54t/m7XonxIQ==","startTime":1589120871},{"expiryTime":1589122671,"tempID":"NCI2zuvgt xLgfq hMBI2cMTT95GBO7gVVeLQzTTYCcp8SvA/Ca+uGVAZHssfQmkMBR9kGxIP92j75qillw==","startTime":1 589121771},{"expiryTime":1589123571,"tempID":"6gdiPwcxVXDtFqelVEFG+VpZVYe8jRnfyNJ+kXb4jSV qLjE6lZCFgw5FwTAdq6/rKbjOFe1hj1ESvbW9aQ==","startTime":1589122671},{"expiryTime":15891244 71,"temp ID":"MnqyH8m5ateY/QX7h6ERrbAq9BTsVSfEpVXDzdX8hxpCuhSpsPvCaZeJQfARxSmzj1nHS+RvqDNNk+ CitQ==","startTime":1589123571},{"expiryTime":1589125371,"tempID":"Op7Nh71xAL9A3rLHARyPjbX OmRuOqLlrqk1SKwI4MITcM5bhkFa/5I7ZPvCUX+3JF7USJZxBCbpdWoPzYw==","startTime":158912447 1},{"expiryTim e":1589126271,"tempID":"phI5U2t9gnDFzU2EA0CLtMnVnoITFlzYAznZJOSh8DswzXdzUibO8AdCAfov3 YSavijqaAVzdzyfmZ1EA==" </pre>		

6.5. SEQ20200500305

PODATNOŚĆ	[Android] Dane wrażliwe – baza danych zawierająca listę odczytanych 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 pobrane z napotkanych urządzeń przechowywane są w nieszyfrowanej bazie danych /data/data/pl.gov.mc.protegosafe/databases/record_database. Atakujący, który uzyska dostęp do systemu plików na urządzeniu może pozyskać identyfikatory uzyskując informacje dotyczące historii kontaktów użytkownika z określonymi urządzeniami i powiązаныmi identyfikatorami.																																																																																																																																																																																																																																																																						
ZALECENIA	Zalecamy wprowadzenie mechanizmu root-detection, który ograniczy problem dostępu do wrażliwych danych na zrootowanych urządzeniach. Zalecamy zastosowanie szyfrowania bazy danych.																																																																																																																																																																																																																																																																						
SZCZEGÓŁY TECHNICZNE	Baza danych sqlite record_database znajduje się w lokalizacji /data/data/pl.gov.mc.protegosafe/databases. Baza nie jest szyfrowana. Tablica record_table zawiera informacje dotyczące czasu rozpoznania, wersji protokołu, tempID, tag organizacji, nazwy urządzeń, wskaźniki rssi oraz txPower. Przykładowa zawartość tablicy record_table widoczna jest poniżej: Table: record_table <table border="1" data-bbox="464 1240 1394 1899"> <thead> <tr> <th>id</th> <th>timestamp</th> <th>v</th> <th>msg</th> <th>org</th> <th>modelP</th> <th>modelC</th> <th>rssi</th> </tr> </thead> <tbody> <tr><td>1</td><td>129</td><td>1588649544594</td><td>2</td><td>xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-83</td></tr> <tr><td>2</td><td>130</td><td>1588649685554</td><td>2</td><td>xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-84</td></tr> <tr><td>3</td><td>131</td><td>1588649832474</td><td>2</td><td>xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-80</td></tr> <tr><td>4</td><td>132</td><td>1588649923120</td><td>2</td><td>xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-83</td></tr> <tr><td>5</td><td>133</td><td>1588650168142</td><td>2</td><td>xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-85</td></tr> <tr><td>6</td><td>134</td><td>1588650272291</td><td>2</td><td>xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-82</td></tr> <tr><td>7</td><td>58</td><td>1588636991899</td><td>2</td><td>wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-80</td></tr> <tr><td>8</td><td>59</td><td>1588637141931</td><td>2</td><td>wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-79</td></tr> <tr><td>9</td><td>60</td><td>1588637279711</td><td>2</td><td>wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-84</td></tr> <tr><td>10</td><td>61</td><td>1588637381780</td><td>2</td><td>wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-79</td></tr> <tr><td>11</td><td>62</td><td>1588637526849</td><td>2</td><td>wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-80</td></tr> <tr><td>12</td><td>63</td><td>1588637717203</td><td>2</td><td>wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-83</td></tr> <tr><td>13</td><td>3</td><td>1588627264011</td><td>2</td><td>u8emrXNohxX96s/meAJfYk73PtkSjwHXoTyXo+N3jfqzGawsE...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-67</td></tr> <tr><td>14</td><td>4</td><td>1588627417907</td><td>2</td><td>u8emrXNohxX96s/meAJfYk73PtkSjwHXoTyXo+N3jfqzGawsE...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-62</td></tr> <tr><td>15</td><td>5</td><td>1588627720542</td><td>2</td><td>u8emrXNohxX96s/meAJfYk73PtkSjwHXoTyXo+N3jfqzGawsE...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-67</td></tr> <tr><td>16</td><td>6</td><td>1588627732662</td><td>2</td><td>u8emrXNohxX96s/meAJfYk73PtkSjwHXoTyXo+N3jfqzGawsE...</td><td>PL_PGS</td><td>SM-G920F</td><td>Redmi Note...</td><td>-57</td></tr> <tr><td>17</td><td>7</td><td>1588627863500</td><td>2</td><td>u8emrXNohxX96s/meAJfYk73PtkSjwHXoTyXo+N3jfqzGawsE...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-61</td></tr> <tr><td>18</td><td>74</td><td>1588640027119</td><td>2</td><td>u0NHr3Tp+BeHi/eTORxKucjuSt4jlt9trY9d5YDh9kYw5ZyAkD...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-79</td></tr> <tr><td>19</td><td>75</td><td>1588640217201</td><td>2</td><td>u0NHr3Tp+BeHi/eTORxKucjuSt4jlt9trY9d5YDh9kYw5ZyAkD...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-80</td></tr> <tr><td>20</td><td>76</td><td>1588640357991</td><td>2</td><td>u0NHr3Tp+BeHi/eTORxKucjuSt4jlt9trY9d5YDh9kYw5ZyAkD...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-84</td></tr> <tr><td>21</td><td>77</td><td>1588640507038</td><td>2</td><td>u0NHr3Tp+BeHi/eTORxKucjuSt4jlt9trY9d5YDh9kYw5ZyAkD...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-79</td></tr> <tr><td>22</td><td>26</td><td>1588631649108</td><td>2</td><td>tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-83</td></tr> <tr><td>23</td><td>27</td><td>1588631694546</td><td>2</td><td>tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-83</td></tr> <tr><td>24</td><td>28</td><td>1588631830370</td><td>2</td><td>tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-84</td></tr> <tr><td>25</td><td>29</td><td>1588631977469</td><td>2</td><td>tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-84</td></tr> <tr><td>26</td><td>30</td><td>1588632272509</td><td>2</td><td>tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-84</td></tr> <tr><td>27</td><td>31</td><td>1588632323015</td><td>2</td><td>tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-84</td></tr> <tr><td>28</td><td>53</td><td>1588636147888</td><td>2</td><td>rIAfn1mP6sWMSMOU0yeZvG9q6F1AieNIRWY0uzEsSbeJmg7r7...</td><td>PL_PGS</td><td>Redmi Note 8 Pro</td><td>SM-G920F</td><td>-79</td></tr> </tbody> </table>			id	timestamp	v	msg	org	modelP	modelC	rssi	1	129	1588649544594	2	xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-83	2	130	1588649685554	2	xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-84	3	131	1588649832474	2	xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-80	4	132	1588649923120	2	xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-83	5	133	1588650168142	2	xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-85	6	134	1588650272291	2	xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-82	7	58	1588636991899	2	wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-80	8	59	1588637141931	2	wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-79	9	60	1588637279711	2	wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-84	10	61	1588637381780	2	wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-79	11	62	1588637526849	2	wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-80	12	63	1588637717203	2	wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-83	13	3	1588627264011	2	u8emrXNohxX96s/meAJfYk73PtkSjwHXoTyXo+N3jfqzGawsE...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-67	14	4	1588627417907	2	u8emrXNohxX96s/meAJfYk73PtkSjwHXoTyXo+N3jfqzGawsE...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-62	15	5	1588627720542	2	u8emrXNohxX96s/meAJfYk73PtkSjwHXoTyXo+N3jfqzGawsE...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-67	16	6	1588627732662	2	u8emrXNohxX96s/meAJfYk73PtkSjwHXoTyXo+N3jfqzGawsE...	PL_PGS	SM-G920F	Redmi Note...	-57	17	7	1588627863500	2	u8emrXNohxX96s/meAJfYk73PtkSjwHXoTyXo+N3jfqzGawsE...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-61	18	74	1588640027119	2	u0NHr3Tp+BeHi/eTORxKucjuSt4jlt9trY9d5YDh9kYw5ZyAkD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-79	19	75	1588640217201	2	u0NHr3Tp+BeHi/eTORxKucjuSt4jlt9trY9d5YDh9kYw5ZyAkD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-80	20	76	1588640357991	2	u0NHr3Tp+BeHi/eTORxKucjuSt4jlt9trY9d5YDh9kYw5ZyAkD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-84	21	77	1588640507038	2	u0NHr3Tp+BeHi/eTORxKucjuSt4jlt9trY9d5YDh9kYw5ZyAkD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-79	22	26	1588631649108	2	tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-83	23	27	1588631694546	2	tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-83	24	28	1588631830370	2	tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-84	25	29	1588631977469	2	tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-84	26	30	1588632272509	2	tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-84	27	31	1588632323015	2	tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-84	28	53	1588636147888	2	rIAfn1mP6sWMSMOU0yeZvG9q6F1AieNIRWY0uzEsSbeJmg7r7...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-79
id	timestamp	v	msg	org	modelP	modelC	rssi																																																																																																																																																																																																																																																																
1	129	1588649544594	2	xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-83																																																																																																																																																																																																																																																															
2	130	1588649685554	2	xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-84																																																																																																																																																																																																																																																															
3	131	1588649832474	2	xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-80																																																																																																																																																																																																																																																															
4	132	1588649923120	2	xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-83																																																																																																																																																																																																																																																															
5	133	1588650168142	2	xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-85																																																																																																																																																																																																																																																															
6	134	1588650272291	2	xuN9eFSrrcFgYgK+zcDvPQmdMYIU872F9jSfbvOFyKWrD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-82																																																																																																																																																																																																																																																															
7	58	1588636991899	2	wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-80																																																																																																																																																																																																																																																															
8	59	1588637141931	2	wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-79																																																																																																																																																																																																																																																															
9	60	1588637279711	2	wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-84																																																																																																																																																																																																																																																															
10	61	1588637381780	2	wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-79																																																																																																																																																																																																																																																															
11	62	1588637526849	2	wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-80																																																																																																																																																																																																																																																															
12	63	1588637717203	2	wYnzDqmkSw3/i4CL9nGTpFT2myr/X0bY0td+3ldGX5WDC5Nj...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-83																																																																																																																																																																																																																																																															
13	3	1588627264011	2	u8emrXNohxX96s/meAJfYk73PtkSjwHXoTyXo+N3jfqzGawsE...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-67																																																																																																																																																																																																																																																															
14	4	1588627417907	2	u8emrXNohxX96s/meAJfYk73PtkSjwHXoTyXo+N3jfqzGawsE...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-62																																																																																																																																																																																																																																																															
15	5	1588627720542	2	u8emrXNohxX96s/meAJfYk73PtkSjwHXoTyXo+N3jfqzGawsE...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-67																																																																																																																																																																																																																																																															
16	6	1588627732662	2	u8emrXNohxX96s/meAJfYk73PtkSjwHXoTyXo+N3jfqzGawsE...	PL_PGS	SM-G920F	Redmi Note...	-57																																																																																																																																																																																																																																																															
17	7	1588627863500	2	u8emrXNohxX96s/meAJfYk73PtkSjwHXoTyXo+N3jfqzGawsE...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-61																																																																																																																																																																																																																																																															
18	74	1588640027119	2	u0NHr3Tp+BeHi/eTORxKucjuSt4jlt9trY9d5YDh9kYw5ZyAkD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-79																																																																																																																																																																																																																																																															
19	75	1588640217201	2	u0NHr3Tp+BeHi/eTORxKucjuSt4jlt9trY9d5YDh9kYw5ZyAkD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-80																																																																																																																																																																																																																																																															
20	76	1588640357991	2	u0NHr3Tp+BeHi/eTORxKucjuSt4jlt9trY9d5YDh9kYw5ZyAkD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-84																																																																																																																																																																																																																																																															
21	77	1588640507038	2	u0NHr3Tp+BeHi/eTORxKucjuSt4jlt9trY9d5YDh9kYw5ZyAkD...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-79																																																																																																																																																																																																																																																															
22	26	1588631649108	2	tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-83																																																																																																																																																																																																																																																															
23	27	1588631694546	2	tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-83																																																																																																																																																																																																																																																															
24	28	1588631830370	2	tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-84																																																																																																																																																																																																																																																															
25	29	1588631977469	2	tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-84																																																																																																																																																																																																																																																															
26	30	1588632272509	2	tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-84																																																																																																																																																																																																																																																															
27	31	1588632323015	2	tFRS6UDq1E2OAH/K70vVzPLNOu4njghAGPVFAi6Lw9kYL2TA...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-84																																																																																																																																																																																																																																																															
28	53	1588636147888	2	rIAfn1mP6sWMSMOU0yeZvG9q6F1AieNIRWY0uzEsSbeJmg7r7...	PL_PGS	Redmi Note 8 Pro	SM-G920F	-79																																																																																																																																																																																																																																																															

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 ankiecie dotyczącej oceny ryzyka zakażenia wraz z wynikiem tej oceny w lokalnej pamięci (local storage) mechanizmu WebView (silnika przeglądarki). Dane te nie są szyfrowane, co w przypadku zainfekowania zrootwanego urządzenia złośliwym oprogramowaniem (lub zainfekowania dowolnego urządzenia złośliwym oprogramowaniem posiadającym funkcjonalność rootowania) może prowadzić do ujawnienia danych medycznych atakującemu.		
ZALECENIA	Zaszifrować wrażliwe dane znajdujące się w /data/data/pl.gov.mc.protegosafe/app_webview/Default/Local Storage/leveldb.		
SZCZEGÓŁY TECHNICZNE	Aplikacja dla Android przechowuje odpowiedzi na pytania z ankiety dotyczącej oceny ryzyka zakażenia wraz z wynikiem tej oceny w lokalnej pamięci, w pamięci lokalnej mechanizmu WebView, zaimplementowanej jako baza danych LevelDB znajdujące się w katalogu /data/data/pl.gov.mc.protegosafe/app_webview/Default/Local Storage/leveldb. Przykładowa zawartość bazy danych widoczna jest poniżej: <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <pre> 'app': '{"onboardingFinished":true,"startScreenShown":true}', 'diagnosis': '{"evidence":[],"inProgress":false,"isLoading":false,"isResetting":true,"question":{},"allQuestions":[]}', 'triage': '{"isLoading":false,"triageLevel":"no_risk","label":"Postpuj zgodnie z zaleceniami epidemiologicznymi.", "description":"Odpowiedzi, których udzieliBe[, nie wskazuj na zaka enie koronawirusem (choroba COVID-19). Stosuj poni sze [rodki zapobiegawcze, by unikn zaka enia. Pamitaj, e Twoje objawy mog wynika tak e z innych chorób i mog wymaga konsultacji lekarskiej - powy szy wywiad jest ukierunkowany na COVID-19. Je[li twoje objawy wydaj si niepokojce, skontaktuj si z lekarzem.", "serious":[]}', 'user': '{"age":29,"bloodGroup":"B+","chronicSicks":[],"name":"Aaa","sex":"male","smokeNumber":null}', ... {"id":"p_15","choice_id":"present"},"triageLevel":"no_risk","label":"Postpuj zgodnie z zaleceniami epidemiologicznymi.", "description":"Odpowiedzi, których udzieliBe[, nie wskazuj na zaka enie koronawirusem (choroba COVID-19). Stosuj poni sze [rodki zapobiegawcze, by unikn zaka enia. Pamitaj, e Twoje objawy mog wynika tak e z innych chorób i mog wymaga konsultacji lekarskiej - powy szy wywiad jest ukierunkowany na COVID-19. Je[li twoje objawy wydaj si niepokojce, skontaktuj si z lekarzem."}}', 'daily': '{"1588586778":{"data":{"temperature":36.5,"runnyNose":"level 1","cough":"level 1","chills":"level 1","musclePain":"level 1","contacts":""}}}', </pre> </div>		

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 nieszyfrowane w pliku <i>/var/mobile/Containers/Data/Application/APP-UUID/Library/Preferences/pl.gov.mc.protegosafe.plist</i> . Atakujący, który uzyska dostęp do systemu plików na urządzeniu może pozyskać identyfikatory, które użytkownik rozgłasza i będzie rozgłaszał w najbliższym czasie.		
ZALECENIA	Zalecamy wprowadzenie mechanizmu jailbreak-detection, który ograniczy problem dostępu do wrażliwych danych na jailbreakowanych urządzeniach. Zalecamy przechowywać tymczasowe identyfikatory w szyfrowanej formie.		
SZCZEGÓŁY TECHNICZNE	Tymczasowe identyfikatory znajdują się w pliku <i>pl.gov.mc.protegosafe.plist</i> w lokalizacji <i>/var/mobile/Containers/Data/Application/APP-UUID/Library/Preferences</i> pod kluczem <code>BROADCAST_MSG</code> oraz <code>BROAD_MSG_ARRAY</code> : <pre> { "ADVT_DATA" = {length = 128, bytes = 0x7b226d70 223a2269 50686f6e 65205822 ... 222c2276 223a327d }; "ADVT_EXPIRY" = "2020-05-11 00:26:43 +0000"; "BROADCAST_MSG" = "i+eVc6nqmQj1h/vmlEaRaJJIS/awzroLjGbvjDY9R8QYR0FPj0vBCx6oDzmlAVFFG611kuQUfM5QV100g="; "BROAD_MSG_ARRAY" = ({ expiryTime = 1589114443; startTime = 1589113543; tempID = "NBnnS0JuMzFUXi8B9JKahYNoH7K3k9kWYkXAaHNf1NGcZfeAHihkY+wii1kH6uZudKMU/mBtLEYq8FFgrg="; }, { expiryTime = 1589115343; startTime = 1589114443; tempID = "gyilln2wLed8uZae60ds+cPtbXe6JsVO789F3eKlmL2kYL/MiCHQ9N2WUnSW4DzgoylWTJJCQlobSpMcx/g="; }, { expiryTime = 1589116243; startTime = 1589115343; tempID = "SnFblCsXlvqAwegb9yXSTBYZwSGmpQZdYaJtYDQw0xvztj8p05m4j7prUijYetsCYoRp0YrixqDhVH7ueg="; }, { expiryTime = 1589117143; startTime = 1589116243; tempID = "nNtDBfYxSIRNWikLvl002mxTG+C5TJGd9p5lpBds3wYUtoy5zNF4xEAMZ379RM3i7+OggXD3GSB8bbgSI"; }) } </pre>		

6.8. SEQ20200500308

PODATNOŚĆ	[iOS] Dane wrażliwe – baza danych zawierająca listę odczytanych 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 pobrane z napotkanych urządzeń przechowywane są w nieszyfrowanej bazie danych /var/mobile/Containers/Data/Application/APP_UUID/Library/Application Support/tracer.sqlite. Atakujący, który uzyska dostęp do systemu plików na urządzeniu może pozyskać identyfikatory uzyskując informacje dotyczące historii kontaktów użytkownika z określonymi urządzeniami i powiązаныmi identyfikatorami.																																																																																																																																																																																																																																																																																																																																																														
ZALECENIA	Zalecamy wprowadzenie mechanizmu jailbreak-detection, który ograniczy problem dostępu do wrażliwych danych na jailbreakowanych urządzeniach. Zalecamy zastosowanie szyfrowania bazy danych.																																																																																																																																																																																																																																																																																																																																																														
SZCZEGÓŁY TECHNICZNE	Baza sqlite tracer.sqlite znajduje się w lokalizacji /var/mobile/Containers/Data/Application/APP-UUID/Library/Application Support. Baza nie jest szyfrowana. Tablica ZENCOUNTER zawiera podobne wpisy jak w przypadku wersji Android. Przykładowa zawartość tablicy ZENCOUNTER widoczna jest poniżej:																																																																																																																																																																																																																																																																																																																																																														
Table: ZENCOUNTER																																																																																																																																																																																																																																																																																																																																																															
<table border="1" style="width: 100%; border-collapse: collapse; font-size: 8px;"> <thead> <tr> <th>Z</th> <th>PK</th> <th>Z_ENT</th> <th>Z_OPT</th> <th>ZV</th> <th>ZRSSI</th> <th>ZTIMESTAMP</th> <th>TXPOWER</th> <th>ZMODELC</th> <th>ZHODELP</th> <th>ZMSG</th> <th>ZORG</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>NULL</td> <td>0.0</td> <td>610444230...</td> <td>0.0</td> <td>NULL</td> <td>NULL</td> <td>Scanning started</td> <td>NULL</td> </tr> <tr> <td>2</td> <td>2</td> <td>1</td> <td>1</td> <td>2</td> <td>-51.0</td> <td>610444231...</td> <td>1.0</td> <td>iPhone X</td> <td>SM-G920F</td> <td>fr4prfG8kjiaFuFwD0yVWjxtZlIm64us1YF2VCysGdZIX+9zFXB2Qzc13ELpPdegwtrO...</td> <td>PL_PGS</td> </tr> <tr> <td>3</td> <td>3</td> <td>1</td> <td>1</td> <td>2</td> <td>-58.0</td> <td>610444231...</td> <td>4.0</td> <td>iPhone X</td> <td>Redmi Note 8 Pro</td> <td>PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...</td> <td>PL_PGS</td> </tr> <tr> <td>4</td> <td>4</td> <td>1</td> <td>1</td> <td>NULL</td> <td>0.0</td> <td>610444240...</td> <td>0.0</td> <td>NULL</td> <td>NULL</td> <td>Scanning stopped</td> <td>NULL</td> </tr> <tr> <td>5</td> <td>5</td> <td>1</td> <td>1</td> <td>NULL</td> <td>0.0</td> <td>610444290...</td> <td>0.0</td> <td>NULL</td> <td>NULL</td> <td>Scanning started</td> <td>NULL</td> </tr> <tr> <td>6</td> <td>6</td> <td>1</td> <td>1</td> <td>2</td> <td>-28.0</td> <td>610444291...</td> <td>1.0</td> <td>iPhone X</td> <td>SM-G920F</td> <td>fr4prfG8kjiaFuFwD0yVWjxtZlIm64us1YF2VCysGdZIX+9zFXB2Qzc13ELpPdegwtrO...</td> <td>PL_PGS</td> </tr> <tr> <td>7</td> <td>7</td> <td>1</td> <td>1</td> <td>2</td> <td>-63.0</td> <td>610444291...</td> <td>4.0</td> <td>iPhone X</td> <td>Redmi Note 8 Pro</td> <td>PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...</td> <td>PL_PGS</td> </tr> <tr> <td>8</td> <td>8</td> <td>1</td> <td>1</td> <td>NULL</td> <td>0.0</td> <td>610444301...</td> <td>0.0</td> <td>NULL</td> <td>NULL</td> <td>Scanning stopped</td> <td>NULL</td> </tr> <tr> <td>9</td> <td>9</td> <td>1</td> <td>1</td> <td>NULL</td> <td>0.0</td> <td>610444350...</td> <td>0.0</td> <td>NULL</td> <td>NULL</td> <td>Scanning started</td> <td>NULL</td> </tr> <tr> <td>10</td> <td>10</td> <td>1</td> <td>1</td> <td>2</td> <td>-62.0</td> <td>610444350...</td> <td>4.0</td> <td>iPhone X</td> <td>Redmi Note 8 Pro</td> <td>PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...</td> <td>PL_PGS</td> </tr> <tr> <td>11</td> <td>11</td> <td>1</td> <td>1</td> <td>2</td> <td>-27.0</td> <td>610444352...</td> <td>1.0</td> <td>iPhone X</td> <td>SM-G920F</td> <td>fr4prfG8kjiaFuFwD0yVWjxtZlIm64us1YF2VCysGdZIX+9zFXB2Qzc13ELpPdegwtrO...</td> <td>PL_PGS</td> </tr> <tr> <td>12</td> <td>12</td> <td>1</td> <td>1</td> <td>NULL</td> <td>0.0</td> <td>610444361...</td> <td>0.0</td> <td>NULL</td> <td>NULL</td> <td>Scanning started</td> <td>NULL</td> </tr> <tr> <td>13</td> <td>13</td> <td>1</td> <td>1</td> <td>NULL</td> <td>0.0</td> <td>610444410...</td> <td>0.0</td> <td>NULL</td> <td>NULL</td> <td>Scanning stopped</td> <td>NULL</td> </tr> <tr> <td>14</td> <td>14</td> <td>1</td> <td>1</td> <td>2</td> <td>-54.0</td> <td>610444411...</td> <td>4.0</td> <td>iPhone X</td> <td>Redmi Note 8 Pro</td> <td>PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...</td> <td>PL_PGS</td> </tr> <tr> <td>15</td> <td>15</td> <td>1</td> <td>1</td> <td>2</td> <td>-23.0</td> <td>610444410...</td> <td>1.0</td> <td>iPhone X</td> <td>SM-G920F</td> <td>fr4prfG8kjiaFuFwD0yVWjxtZlIm64us1YF2VCysGdZIX+9zFXB2Qzc13ELpPdegwtrO...</td> <td>PL_PGS</td> </tr> <tr> <td>16</td> <td>16</td> <td>1</td> <td>1</td> <td>NULL</td> <td>0.0</td> <td>610444421...</td> <td>0.0</td> <td>NULL</td> <td>NULL</td> <td>Scanning started</td> <td>NULL</td> </tr> <tr> <td>17</td> <td>17</td> <td>1</td> <td>1</td> <td>NULL</td> <td>0.0</td> <td>610444470...</td> <td>0.0</td> <td>NULL</td> <td>NULL</td> <td>Scanning stopped</td> <td>NULL</td> </tr> <tr> <td>18</td> <td>18</td> <td>1</td> <td>1</td> <td>2</td> <td>-61.0</td> <td>610444471...</td> <td>1.0</td> <td>iPhone X</td> <td>SM-G920F</td> <td>fr4prfG8kjiaFuFwD0yVWjxtZlIm64us1YF2VCysGdZIX+9zFXB2Qzc13ELpPdegwtrO...</td> <td>PL_PGS</td> </tr> <tr> <td>19</td> <td>19</td> <td>1</td> <td>1</td> <td>2</td> <td>-58.0</td> <td>610444472...</td> <td>4.0</td> <td>iPhone X</td> <td>Redmi Note 8 Pro</td> <td>PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...</td> <td>PL_PGS</td> </tr> <tr> <td>20</td> <td>20</td> <td>1</td> <td>1</td> <td>NULL</td> <td>0.0</td> <td>610444481...</td> <td>0.0</td> <td>NULL</td> <td>NULL</td> <td>Scanning stopped</td> <td>NULL</td> </tr> <tr> <td>21</td> <td>21</td> <td>1</td> <td>1</td> <td>NULL</td> <td>0.0</td> <td>610444530...</td> <td>0.0</td> <td>NULL</td> <td>NULL</td> <td>Scanning started</td> <td>NULL</td> </tr> <tr> <td>22</td> <td>22</td> <td>1</td> <td>1</td> <td>2</td> <td>-65.0</td> <td>610444530...</td> <td>4.0</td> <td>iPhone X</td> <td>Redmi Note 8 Pro</td> <td>PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...</td> <td>PL_PGS</td> </tr> <tr> <td>23</td> <td>23</td> <td>1</td> <td>1</td> <td>2</td> <td>-34.0</td> <td>610444532...</td> <td>1.0</td> <td>iPhone X</td> <td>SM-G920F</td> <td>v2pTtsb/5bZDcauegoMShhbR5cOmNPVFW7/jwNcG3YE+52m4cWB55bPRT6v6Qn...</td> <td>PL_PGS</td> </tr> <tr> <td>24</td> <td>24</td> <td>1</td> <td>1</td> <td>NULL</td> <td>0.0</td> <td>610444541...</td> <td>0.0</td> <td>NULL</td> <td>NULL</td> <td>Scanning stopped</td> <td>NULL</td> </tr> <tr> <td>25</td> <td>25</td> <td>1</td> <td>1</td> <td>NULL</td> <td>0.0</td> <td>610444590...</td> <td>0.0</td> <td>NULL</td> <td>NULL</td> <td>Scanning started</td> <td>NULL</td> </tr> <tr> <td>26</td> <td>26</td> <td>1</td> <td>1</td> <td>2</td> <td>-26.0</td> <td>610444590...</td> <td>1.0</td> <td>iPhone X</td> <td>SM-G920F</td> <td>v2pTtsb/5bZDcauegoMShhbR5cOmNPVFW7/jwNcG3YE+52m4cWB55bPRT6v6Qn...</td> <td>PL_PGS</td> </tr> <tr> <td>27</td> <td>27</td> <td>1</td> <td>1</td> <td>2</td> <td>-51.0</td> <td>610444591...</td> <td>4.0</td> <td>iPhone X</td> <td>Redmi Note 8 Pro</td> <td>PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...</td> <td>PL_PGS</td> </tr> <tr> <td>28</td> <td>28</td> <td>1</td> <td>1</td> <td>NULL</td> <td>0.0</td> <td>610444601...</td> <td>0.0</td> <td>NULL</td> <td>NULL</td> <td>Scanning stopped</td> <td>NULL</td> </tr> </tbody> </table>				Z	PK	Z_ENT	Z_OPT	ZV	ZRSSI	ZTIMESTAMP	TXPOWER	ZMODELC	ZHODELP	ZMSG	ZORG	1	1	1	1	NULL	0.0	610444230...	0.0	NULL	NULL	Scanning started	NULL	2	2	1	1	2	-51.0	610444231...	1.0	iPhone X	SM-G920F	fr4prfG8kjiaFuFwD0yVWjxtZlIm64us1YF2VCysGdZIX+9zFXB2Qzc13ELpPdegwtrO...	PL_PGS	3	3	1	1	2	-58.0	610444231...	4.0	iPhone X	Redmi Note 8 Pro	PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...	PL_PGS	4	4	1	1	NULL	0.0	610444240...	0.0	NULL	NULL	Scanning stopped	NULL	5	5	1	1	NULL	0.0	610444290...	0.0	NULL	NULL	Scanning started	NULL	6	6	1	1	2	-28.0	610444291...	1.0	iPhone X	SM-G920F	fr4prfG8kjiaFuFwD0yVWjxtZlIm64us1YF2VCysGdZIX+9zFXB2Qzc13ELpPdegwtrO...	PL_PGS	7	7	1	1	2	-63.0	610444291...	4.0	iPhone X	Redmi Note 8 Pro	PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...	PL_PGS	8	8	1	1	NULL	0.0	610444301...	0.0	NULL	NULL	Scanning stopped	NULL	9	9	1	1	NULL	0.0	610444350...	0.0	NULL	NULL	Scanning started	NULL	10	10	1	1	2	-62.0	610444350...	4.0	iPhone X	Redmi Note 8 Pro	PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...	PL_PGS	11	11	1	1	2	-27.0	610444352...	1.0	iPhone X	SM-G920F	fr4prfG8kjiaFuFwD0yVWjxtZlIm64us1YF2VCysGdZIX+9zFXB2Qzc13ELpPdegwtrO...	PL_PGS	12	12	1	1	NULL	0.0	610444361...	0.0	NULL	NULL	Scanning started	NULL	13	13	1	1	NULL	0.0	610444410...	0.0	NULL	NULL	Scanning stopped	NULL	14	14	1	1	2	-54.0	610444411...	4.0	iPhone X	Redmi Note 8 Pro	PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...	PL_PGS	15	15	1	1	2	-23.0	610444410...	1.0	iPhone X	SM-G920F	fr4prfG8kjiaFuFwD0yVWjxtZlIm64us1YF2VCysGdZIX+9zFXB2Qzc13ELpPdegwtrO...	PL_PGS	16	16	1	1	NULL	0.0	610444421...	0.0	NULL	NULL	Scanning started	NULL	17	17	1	1	NULL	0.0	610444470...	0.0	NULL	NULL	Scanning stopped	NULL	18	18	1	1	2	-61.0	610444471...	1.0	iPhone X	SM-G920F	fr4prfG8kjiaFuFwD0yVWjxtZlIm64us1YF2VCysGdZIX+9zFXB2Qzc13ELpPdegwtrO...	PL_PGS	19	19	1	1	2	-58.0	610444472...	4.0	iPhone X	Redmi Note 8 Pro	PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...	PL_PGS	20	20	1	1	NULL	0.0	610444481...	0.0	NULL	NULL	Scanning stopped	NULL	21	21	1	1	NULL	0.0	610444530...	0.0	NULL	NULL	Scanning started	NULL	22	22	1	1	2	-65.0	610444530...	4.0	iPhone X	Redmi Note 8 Pro	PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...	PL_PGS	23	23	1	1	2	-34.0	610444532...	1.0	iPhone X	SM-G920F	v2pTtsb/5bZDcauegoMShhbR5cOmNPVFW7/jwNcG3YE+52m4cWB55bPRT6v6Qn...	PL_PGS	24	24	1	1	NULL	0.0	610444541...	0.0	NULL	NULL	Scanning stopped	NULL	25	25	1	1	NULL	0.0	610444590...	0.0	NULL	NULL	Scanning started	NULL	26	26	1	1	2	-26.0	610444590...	1.0	iPhone X	SM-G920F	v2pTtsb/5bZDcauegoMShhbR5cOmNPVFW7/jwNcG3YE+52m4cWB55bPRT6v6Qn...	PL_PGS	27	27	1	1	2	-51.0	610444591...	4.0	iPhone X	Redmi Note 8 Pro	PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...	PL_PGS	28	28	1	1	NULL	0.0	610444601...	0.0	NULL	NULL	Scanning stopped	NULL
Z	PK	Z_ENT	Z_OPT	ZV	ZRSSI	ZTIMESTAMP	TXPOWER	ZMODELC	ZHODELP	ZMSG	ZORG																																																																																																																																																																																																																																																																																																																																																				
1	1	1	1	NULL	0.0	610444230...	0.0	NULL	NULL	Scanning started	NULL																																																																																																																																																																																																																																																																																																																																																				
2	2	1	1	2	-51.0	610444231...	1.0	iPhone X	SM-G920F	fr4prfG8kjiaFuFwD0yVWjxtZlIm64us1YF2VCysGdZIX+9zFXB2Qzc13ELpPdegwtrO...	PL_PGS																																																																																																																																																																																																																																																																																																																																																				
3	3	1	1	2	-58.0	610444231...	4.0	iPhone X	Redmi Note 8 Pro	PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...	PL_PGS																																																																																																																																																																																																																																																																																																																																																				
4	4	1	1	NULL	0.0	610444240...	0.0	NULL	NULL	Scanning stopped	NULL																																																																																																																																																																																																																																																																																																																																																				
5	5	1	1	NULL	0.0	610444290...	0.0	NULL	NULL	Scanning started	NULL																																																																																																																																																																																																																																																																																																																																																				
6	6	1	1	2	-28.0	610444291...	1.0	iPhone X	SM-G920F	fr4prfG8kjiaFuFwD0yVWjxtZlIm64us1YF2VCysGdZIX+9zFXB2Qzc13ELpPdegwtrO...	PL_PGS																																																																																																																																																																																																																																																																																																																																																				
7	7	1	1	2	-63.0	610444291...	4.0	iPhone X	Redmi Note 8 Pro	PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...	PL_PGS																																																																																																																																																																																																																																																																																																																																																				
8	8	1	1	NULL	0.0	610444301...	0.0	NULL	NULL	Scanning stopped	NULL																																																																																																																																																																																																																																																																																																																																																				
9	9	1	1	NULL	0.0	610444350...	0.0	NULL	NULL	Scanning started	NULL																																																																																																																																																																																																																																																																																																																																																				
10	10	1	1	2	-62.0	610444350...	4.0	iPhone X	Redmi Note 8 Pro	PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...	PL_PGS																																																																																																																																																																																																																																																																																																																																																				
11	11	1	1	2	-27.0	610444352...	1.0	iPhone X	SM-G920F	fr4prfG8kjiaFuFwD0yVWjxtZlIm64us1YF2VCysGdZIX+9zFXB2Qzc13ELpPdegwtrO...	PL_PGS																																																																																																																																																																																																																																																																																																																																																				
12	12	1	1	NULL	0.0	610444361...	0.0	NULL	NULL	Scanning started	NULL																																																																																																																																																																																																																																																																																																																																																				
13	13	1	1	NULL	0.0	610444410...	0.0	NULL	NULL	Scanning stopped	NULL																																																																																																																																																																																																																																																																																																																																																				
14	14	1	1	2	-54.0	610444411...	4.0	iPhone X	Redmi Note 8 Pro	PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...	PL_PGS																																																																																																																																																																																																																																																																																																																																																				
15	15	1	1	2	-23.0	610444410...	1.0	iPhone X	SM-G920F	fr4prfG8kjiaFuFwD0yVWjxtZlIm64us1YF2VCysGdZIX+9zFXB2Qzc13ELpPdegwtrO...	PL_PGS																																																																																																																																																																																																																																																																																																																																																				
16	16	1	1	NULL	0.0	610444421...	0.0	NULL	NULL	Scanning started	NULL																																																																																																																																																																																																																																																																																																																																																				
17	17	1	1	NULL	0.0	610444470...	0.0	NULL	NULL	Scanning stopped	NULL																																																																																																																																																																																																																																																																																																																																																				
18	18	1	1	2	-61.0	610444471...	1.0	iPhone X	SM-G920F	fr4prfG8kjiaFuFwD0yVWjxtZlIm64us1YF2VCysGdZIX+9zFXB2Qzc13ELpPdegwtrO...	PL_PGS																																																																																																																																																																																																																																																																																																																																																				
19	19	1	1	2	-58.0	610444472...	4.0	iPhone X	Redmi Note 8 Pro	PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...	PL_PGS																																																																																																																																																																																																																																																																																																																																																				
20	20	1	1	NULL	0.0	610444481...	0.0	NULL	NULL	Scanning stopped	NULL																																																																																																																																																																																																																																																																																																																																																				
21	21	1	1	NULL	0.0	610444530...	0.0	NULL	NULL	Scanning started	NULL																																																																																																																																																																																																																																																																																																																																																				
22	22	1	1	2	-65.0	610444530...	4.0	iPhone X	Redmi Note 8 Pro	PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...	PL_PGS																																																																																																																																																																																																																																																																																																																																																				
23	23	1	1	2	-34.0	610444532...	1.0	iPhone X	SM-G920F	v2pTtsb/5bZDcauegoMShhbR5cOmNPVFW7/jwNcG3YE+52m4cWB55bPRT6v6Qn...	PL_PGS																																																																																																																																																																																																																																																																																																																																																				
24	24	1	1	NULL	0.0	610444541...	0.0	NULL	NULL	Scanning stopped	NULL																																																																																																																																																																																																																																																																																																																																																				
25	25	1	1	NULL	0.0	610444590...	0.0	NULL	NULL	Scanning started	NULL																																																																																																																																																																																																																																																																																																																																																				
26	26	1	1	2	-26.0	610444590...	1.0	iPhone X	SM-G920F	v2pTtsb/5bZDcauegoMShhbR5cOmNPVFW7/jwNcG3YE+52m4cWB55bPRT6v6Qn...	PL_PGS																																																																																																																																																																																																																																																																																																																																																				
27	27	1	1	2	-51.0	610444591...	4.0	iPhone X	Redmi Note 8 Pro	PRGieShujhLZEwXhk1j0P8MAXFZUm65zArpvWBdCQs3r4zm+/5MC12wRpZ0/139HK...	PL_PGS																																																																																																																																																																																																																																																																																																																																																				
28	28	1	1	NULL	0.0	610444601...	0.0	NULL	NULL	Scanning stopped	NULL																																																																																																																																																																																																																																																																																																																																																				

6.9. SEQ20200500309

PODATNOŚĆ	[Android] Brak zaimplementowanego mechanizmu certificate-pinning	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 <code>networ_securtiy_config.xml</code> zawierający hashe kluczy publicznych wykorzystywanych do realizacji certificate pinning.		
SZCZEGÓŁY TECHNICZNE	Połączenia pomiędzy aplikacjami ProtegoSafe a serwerem <code>https://safesafe.app</code> ładowanym w komponencie WebView (zawierającym widoczną dla użytkownika logikę aplikacji) są zabezpieczone przy użyciu protokołu HTTPS. Aplikacje nie implementują jednak zwiększającego bezpieczeństwa mechanizmu certificate pinning. Brak certificate pinningu może prowadzić do ataków MITM w przypadku zainfekowania zrootwanego lub jailbreakowanego urządzenia złośliwym oprogramowaniem. Przykład wykorzystania podatności dostępny jest w opisie podatności SEQ20200500310.		

6.10. SEQ20200500310

<p>PODATNOŚĆ</p>	<p>[iOS] Brak zaimplementowanego mechanizmu certificate-pinning</p>	<p>PRIORYTET</p>	<p>ŚREDNI</p>
<p>CVSS VECTOR</p>	<p>AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N</p>	<p>CVSS:3.0 base score</p>	<p>5.9</p>
<p>OPIS</p>	<p>Aplikacja nie implementuje zwiększającego bezpieczeństwa mechanizmu certificate pinning. Brak zaimplementowanego mechanizmu może prowadzić do ataków MITM w przypadku zainfekowania zrootwanego urządzenia złośliwym oprogramowaniem.</p>		
<p>ZALECENIA</p>	<p>W przypadku wykorzystania biblioteki Alamofire wykorzystać klasę ServerTrustManager. W przypadku NSURLSession, wykorzystać URLSession:didReceiveChallenge:completionHandler:delegate.</p>		
<p>SZCZEGÓŁY TECHNICZNE</p>	<p>Połączenia pomiędzy aplikacjami ProtegoSafe a serwerem https://safesafe.app ładowanym w komponencie WebView (zawierającym widoczną dla użytkownika logikę aplikacji) są zabezpieczone przy użyciu protokołu HTTPS. Aplikacje nie implementują jednak zwiększającego bezpieczeństwa mechanizmu certificate pinning. Brak certificate pinningu może prowadzić do ataków MITM w przypadku zainfekowania zrootwanego lub jailbreakowanego urządzenia złośliwym oprogramowaniem.</p> <p>Przykład wykorzystania podatności jest widoczny poniżej - odpowiedź z oceną stanu zdrowia została podmieniona:</p> <div data-bbox="730 1332 1125 1951" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> </div>		

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 zapasowych. Dla aplikacji Android w pliku AndroidManifest.xml poprzez zmianę flagi <i>allowBackup</i> na <i>false</i> (<code>android:allowBackup="false"</code>) lub stworzyć reguły backupu wyłączające z niego local storage. Dla aplikacji iOS poprzez wykorzystanie API <code>isExcludedFromBackup()</code> wyłączyć możliwość backupowania plików zawierających wrażliwe dane.		
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	<p>Aplikacje dla systemów Android oraz iOS wykorzystują zegar systemowy jako referencyjny do określenia czasu ważności zapisanych identyfikatorów tymczasowych. Zegar systemowy może być dowolnie modyfikowany przez użytkownika lub zmodyfikowany bez wiedzy użytkownika np. poprzez mechanizm NITZ - uzyskiwania nazwy usługodawcy GSM oraz daty i godziny aktualnej strefy czasowej. Modyfikacje czasu systemowego pozwalają w omawianym przypadku na usunięcie wszystkich rekordów tymczasowych identyfikatorów zapisanych w bazie lub wstrzymać usuwanie przestarzałych identyfikatorów.</p>		
ZALECENIA	<p>Zalecamy porzucić wykorzystanie czasu systemowego na rzecz synchronizacji czasu poprzez protokół NTP, Network Time Protocol. Klient NTP powinien zostać zaimplementowany w aplikacji ProteGo Safe, a wszystkie wrażliwe na zmiany czasu operacje powinny wykorzystywać NTP do pobrania aktualnego czasu.</p>		
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 danych tracer.sqlite starsze niż trzy tygodnie nie są usuwane.		
ZALECENIA	Dodać logikę usuwającą przestarzałe identyfikatory wykorzystując protokół NTP jako źródło czasu.		
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	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 biblioteki 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 powielić (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	<p>W przypadku przekazania poprawnego kodu PIN endpoint /getAccessToken zwraca token JWT w polu <i>accessToken</i>, jak na przykładzie przedstawionym poniżej:</p> <pre> {"result":{"accessToken":"eyJhbGciOiJIUzUxMiIsInR5cCI6IkpXVCJ9.eyJjb2RlIjoiaUJZODAwIiwiaWF0IjoxNTkxMTg3Njc1LCJleHAiOjE1OTExODk0NzUslmp0aSI6ImIixZGQ3NGViLWVlODgtNDU0OS04YWQ0LTQ1MmVZkODRhNDJkZCJ9.ejjcwnaz2PtWWFAya9zCEzLuR_2yI9KTLZIZY-veIYJ3PbztcN9-CRgQx7gim3ra9XcKfNbxks8RNKXlvROvw"} </pre> <p>W przypadku przekazania niepoprawnego kodu PIN endpoint /getAccessToken zwraca błąd jak na przykładzie poniżej:</p> <pre> {"error":{"message":"Invalid code","status":"NOT_FOUND"}} </pre>		

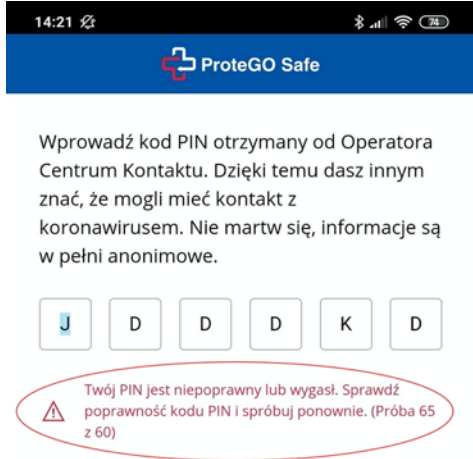
6.17. SEQ20200600203

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

<p>PODATNOŚĆ</p>	<p>[iOS] Możliwość obejścia mechanizmu ograniczenia ilości prób wpisania kodu PIN</p>	<p>PRIORYTET</p>	<p>WYSOKI</p>
<p>CVSS VECTOR</p>	<p>AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:L</p>	<p>CVSS:3.0 base score</p>	<p>7.2</p>
<p>OPIS</p>	<p>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).</p> <p>Walidacja okresu czasu, po jakim użytkownik może wykonać ponowne próby wpisania kodu PIN, bazuje na czasie systemowym urządzenia, który może zostać dowolnie zmodyfikowany przez użytkownika.</p> <p>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.</p> <p>Zauważono również, że licznik ilości prób nie jest zaimplementowany poprawnie co widać na załączonym zrzucie ekranu w kolejnej sekcji.</p>		
<p>ZALECENIA</p>	<p>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.</p>		
<p>SZCZEGÓŁY TECHNICZNE</p>	 <p>00:46</p> <p>ProteGO Safe</p> <p>Wprowadź kod PIN otrzymany od Operatora Centrum Kontaktów. Dzięki temu dasz innym znać, że mogli mieć kontakt z koronawirusem. Nie martw się, informacje są w pełni anonimowe.</p> <p>J D D N J D</p> <p>Twój PIN jest niepoprawny lub wygasł. Sprawdź poprawność kodu PIN i spróbuj ponownie. (Próba 135 z 60)</p>		

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	<p>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).</p> <p>Walidacja okresu czasu, po jakim użytkownik może wykonać ponowne próby wpisania kodu PIN, bazuje na czasie systemowym urządzenia, który może zostać dowolnie zmodyfikowany przez użytkownika.</p> <p>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.</p> <p>Zauważono również, że licznik ilości prób nie jest zaimplementowany poprawnie co widać na załączonym zrzucie ekranu w kolejnej sekcji.</p>		
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	 <p>The screenshot shows the ProteGO Safe PIN entry interface. At the top, the time is 14:21. Below the ProteGO Safe logo, there is a message: "Wprowadź kod PIN otrzymany od Operatora Centrum Kontaktów. Dzięki temu dasz innym znać, że mogli mieć kontakt z koronawirusem. Nie martw się, informacje są w pełni anonimowe." Below this message is a PIN input field with six buttons: J, D, D, D, K, D. At the bottom, a red error message is circled: "Twój PIN jest niepoprawny lub wygasł. Sprawdź poprawność kodu PIN i spróbuj ponownie. (Próba 65 z 60)".</p>		

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	<p>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.</p> <p>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.</p> <p>Dobłą 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.</p> <p>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.</p>		
ZALECENIA	<p>Nagłówek ustawiony dla wszystkich odpowiedzi z serwera z godnie z poniższym:</p> <pre> Strict-Transport-Security: max-age:31536000; includeSubDomains; preload X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block </pre>		

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-oeLEdka2vWl9yVxbTN4fBQZppi0"
Function-Execution-Id: lhjhs551jz6
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 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:

