the **apps** co.

mobisec

WINNERS PLAY IT RIGHT.

28/05/2020

Oggetto dell'analisi

Questo documento di analisi è stato redatto per la società **BENDING SPOONS S.P.A.** in merito alla loro applicazione IMMUNI per i seguenti sistemi operativi:

- **Android**, versione app **0.0.1** – *Link allo Store non disponibile*;
- **iOS**, versione app **1.0** – *Link allo Store non disponibile*;

I test si sono svolti a partire dalla data **21/05/2020** nella sede Mobisec di **TREVISO**.

Vista la presenza di più di un sistema operativo, si ricorda che lo score di sicurezza finale assegnato sarà una media tra i vari risultati e che in coda al documento sarà possibile avere visione anche dei punteggi divisi per singolo OS.

Metodologia di analisi

La procedura di analisi Mobisec dedicata al security assessment delle app mobile viene eseguita con approccio **black-box**, ovvero partendo solamente dal pacchetto di installazione dell'app così come viene scaricato da un normale utente dagli store Apple e Google.

L'analisi inizia con una prima fase di raccolta delle informazioni, tracciamento dei dati e studio dell'architettura applicativa utilizzando dispositivi di mercato altamente personalizzati nel laboratorio Mobisec; su questi device vengono infatti installate delle estensioni del kernel dei sistemi operativi iOS e Android che rappresentano la parte client del software **Mobisec Dynamic Mobile Security Analysis**.

Questa *kernel extension* si occupa di registrare tutti i dati delle operazioni e delle comunicazioni eseguite dall'applicazione in test e spedirle alla controparte server che è in ascolto nella stessa rete interna del client, permettendo così un tracciamento avanzato sia dei dati utilizzati che dei metodi sfruttati per la loro gestione.

Punteggi e domini

A tutte le potenziali vulnerabilità trovate da Mobisec viene assegnato un punteggio e un livello di rischio tramite il sistema **CVSS 3.1**, quindi questi dati vengono forniti all'azienda committente assieme a dei suggerimenti su come applicare una risoluzione; dopo le loro attuazioni i test vengono ripetuti, aggiornando i punteggi e i livelli delle vulnerabilità laddove si sia applicata una mitigazione o rimuovendole dalla lista qualora oggetto di correzione.

Mobisec ha diviso i potenziali problemi di sicurezza in cui le app mobile incorrono in cinque domini principali e va ad assegnare ad ognuno di questi un punteggio da 1 a 5, senza decimali, dove più è alto il numero maggiore è il livello di sicurezza garantito nel dominio:

- **Presence of user data** – Più dati dell'utente l'applicazione tratta, più potenzialmente è a rischio. Il dominio valuta la mole di dati personali, confidenziali e sensibili che può essere rubata o compromessa sfruttando le vulnerabilità note, soppesando anche la complessità d'attacco.

- **Network communications** – Viene valutata la quantità e la qualità delle connessioni effettuate con tecnologie wireless dal dispositivo. Sebbene principalmente i rilevamenti interessino la connessione dati a Internet, questo dominio comprende anche eventuali scambi dati via Bluetooth e NFC.
- **Filesystem** – Le app scrivono continuamente dati nel filesystem in file di preferenze, download, cache, database, ecc. Il dominio legato al filesystem valuta la sicurezza applicata a questi dati salvati nella memoria del device.
- **Data exchange** – Tutte le volte che l'app scambia i dati in suo possesso o quelli inseriti dall'utente con altre app, con particolari processi del filesystem o anche con i server, viene controllata la capacità dell'app e dell'intero sistema di evitare injection, tampering e tainting dei dati.
- **Codebase** – Viene valutato il codice dell'applicazione, assicurandosi venga evitato l'uso di classi e metodi deprecati, librerie insicure, permessi inutilizzati, metodi di crittografia deboli ed altri *flaw* di sicurezza che possano esporre l'app ad attacchi dovuti da una mancata ottimizzazione del suo codice.

mobisec

Presence of user data

Presence of user data

L'applicazione utilizza il framework Apple/Google per la notifica dell'esposizione alla Covid-19, il quale sfrutta un sistema di scambio *token* via Bluetooth completamente anonimi e non riconducibili esplicitamente alla persona o al device cui sono associati.
L'app non fa uso di alcun dato utente personale, privato o sensibile e in caso di accertata infezione dal virus, la comunicazione della stessa è sotto esplicita scelta dell'utente con l'ausilio e la certificazione di un operatore sanitario. Questo evento tuttavia non riporta alcun dato personale nei sistemi di gestione di tracciamento dell'esposizione, limitandosi a comunicare al server la lista dei propri *token* (come sempre anonimi) che risulteranno quindi appartenenti a un infetto, permettendo agli altri utenti di eseguire in automatico un controllo tra i *token* dei dispositivi che hanno incrociato e la lista dei *token* segnalati come infetti.
L'unico dato che viene comunicato ai server di gestione del tracciamento (localizzati in Italia e non appartenenti ad Apple o Google) è la provincia di residenza, utile al governo per gestire stime e spostamenti in caso di infezione.

Punteggio finale

mobisec

NETWORK COMMUNICATIONS

Network communications

Tutte le comunicazioni web avvengono su canali HTTPS sicuri utilizzando come protocollo di sicurezza il TLS alla sua versione 1.3; i certificati installati sul server sono validi e la presenza di certificate pinning lato device rende le connessioni ancora più sicure evitando ogni possibilità di semplici attacchi di tipo Man In The Middle (MITM) che altrimenti con la semplice abilitazione di un proxy di rete sarebbero in grado di avere accesso ai contenuti delle comunicazioni, permettendo sniffing ed injection di dati.
Le comunicazioni Bluetooth avvengono in maniera automatica quando due device con installata l'applicazione sono in prossimità l'uno dell'altro; quando ciò accade i device si scambiano degli hash univoci che in caso di contrazione del Covid-19 vengono poi riutilizzati dal sistema di tracciamento dei contatti; questi hash sono stringhe alfanumeriche calcolate tramite algoritmi matematici in una sequenza di lettere e numeri che, per definizione, non può essere poi calcolata al contrario per riottenere i dati di partenza, rendendo di fatto ogni dato scambiato completamente anonimo.
L'applicazione non fa uso o richiesta d'uso della tecnologia NFC.

Punteggio finale

mobisec

Filesystem

Filesystem

La gestione del filesystem dell'applicazione si limita alla sandbox applicativa, ovvero un'area di memoria del device riservata alla singola app a cui nessun'altra applicazione ha accesso.
In questo spazio dedicato l'app comunque non salva alcun dato personale dell'utente in maniera esplicita, limitandosi ad avere in chiaro al suo interno solamente una cache tecnica con alcuni parametri di setup, utile ad ottimizzare il quantitativo di traffico internet generato dal device.
Il dato relativo alla provincia di residenza invece è salvato in sandbox ma risulta criptato, pertanto inaccessibile, se non utilizzando una chiave di decifratura che solamente l'app possiede e che sfrutta quando l'utente cambia il dato della provincia o quando deve comunicarla in remoto per la segnalazione dell'infezione.

Punteggio finale

mobisec

DATA EXCHANGE

Data exchange

I dati di esposizione, di tracking e di contatto sono tutti quanti scambiati via Bluetooth, anonimizzati e sfruttando le librerie dei sistemi operativi proprietari Apple/Google per la gestione dei token.
L'integrità delle comunicazioni client-server per la segnalazione del contagio è assicurata da un'autorizzazione rilasciata da un operatore sanitario, rendendo pressoché impossibile l'injection di dati fittizi nel database dei positivi.
Le comunicazioni intra-processo avvengono solamente tra l'app e librerie del sistema operativo, nello specifico con il framework Apple/Google, segregando così l'app da attacchi provenienti da altre fonti.

Punteggio finale

mobisec

Codebase

Codebase - Android

Il codice dell'applicazione Android presenta pochissimi rischi per la sicurezza. Tutti i permessi richiesti dall'app (accesso alla rete, bluetooth, esecuzione in primo piano e prevenzione dallo spegnimento dello schermo) sono tutti fondamentali al corretto funzionamento della stessa e ne viene fatto un uso ponderato e pesato sulle reali necessità.
L'applicazione espone anche alcuni *receiver*, servizi interni esposti ad altri processi in esecuzione sullo stesso sistema, che vengono richiamati in particolari momenti (ad esempio all'accensione o al riavvio del device) o su richiesta di altre app e che eseguono operazioni a nome dell'app stessa. Questi *receiver* risultano adeguatamente protetti e confinati ai casi d'uso previsti grazie ad una corretta implementazione dei controlli nel codice.
L'app non fa uso di metodi o classi deprecate, implementa solo gli URL necessari al suo corretto funzionamento ed è priva di librerie di tracking ed analytics, assicurando così per definizione che nessun dato dell'utente sia esposto a terze parti.

Punteggio finale

Codebase - iOS

Il codice scritto per l'app iOS presenta pochissimi rischi per la sicurezza.
L'applicazione non richiede alcun permesso legato all'hardware del device, limitandosi ad assicurarsi che l'utente accetti nella privacy la condivisione dei dati per il tracciamento dell'esposizione al Covid-19.
Non ci sono eccezioni alla sicurezza legate ai requisiti minimi di connessione, e l'app è stata compilata con tutti i possibili flag di protezione agli attacchi di basso livello legati allo sfruttamento della memoria RAM, limitando i possibili danni che un exploit di quel tipo potrebbe generare.
Tutti i domini presenti nel codice di cui l'app fa uso sono stati controllati e risultano sicuri, così come le librerie e i framework.

Punteggio finale

mobisec

Valutazione finale

Punteggio finale

98.6 / 100

PRESENCE OF USER DATA

NETWORK COMMUNICATIONS

FILESYSTEM

DATA EXCHANGE

CODEBASE