Certificat d’audit

Applications STID MOBILE ID Android et iOS + Plateforme Web

PHONESEC

Version du document

Période d'audit	Mars 2018	
Auditeur	Younes Benzagmout @Phonesec	Expert sécurité
Validation	Pascal CAPUANO @Phonesec	Directeur des projets fraude et sécurité
Lieu	France	

Phonesec est une entreprise labélisée France Cybercecurity

1. PERIMETRE ET CONDITIONS GENERALES DES TESTS

Le périmètre de la prestation est défini par le lot de fonctionnalités accessibles via l'application STID MOBILE ID en version 1.0.8 (0.8) pour la plateforme iOS, et v1.1.129d pour la plateforme Android. La plateforme Web vers laquelle pointent les deux applications fait partie du périmètre, cette plateforme étant au moment des tests, destinée à la recette technique et sécurité, convenue comme étant iso à la production.

Ce certificat présente la méthodologie et l'appréciation globale des résultats d'audit.

2. METHODOLOGIE APPLICATIONS CLIENTS

L'application a profité d'une analyse statique et d'une analyse dynamique, flux inclus. Au regard des fonctionnalités de l'application, le plan de test ci-après a été retenu. Chaque test fait l'objet d'un ou plusieurs contrôles selon les exigences de l'analyse.

2.1. Analyse statique

1	Recherche de ressources sensibles dans le package d'installation
2	Méthodologie de requête sur la base de données
3	Sécurisation des appels aux interfaces
4	Usage du clipboard
5	Sécurité des algorithmes de chiffrement
6	Sécurité des algorithmes de hachage
7	Sécurisation de la clé de chiffrement
8	Utilisation de la clé chiffrement
9	Obfuscation du code
10	Vérification du certificat de signature

2.2. Analyse dynamique

1	Stockage en mémoire
2	Stockage de données sensibles dans des fichiers « préférences »
3	Stockage dans des bases de données
4	Création de fichiers contenant des données sensibles
5	Méthode d'authentification
6	Méthode d'autorisation
7	Schéma d'authentification
8	Contrôle de l'authentification
9	Contrôle de l'autorisation
10	Identification
11	Protection de l'identifiant
12	Filtrage des données soumises aux interfaces
13	Contrôle des accès aux interfaces de l'application
14	Utilisation des composants web

15	Logue des données
16	Gestion des exceptions
17	Image de cache en sortie de l'application
18	Gestion des fichiers temporaires
19	Masquage des champs sensibles
20	Auto correction/complétion
21	Protection des clés de chiffrement
22	Contrôle du système (root / jailbreak)
23	Accès aux données privées
24	Utilisation du Webview
25	Application debugging
26	Application Backup

2.3. Analyse de flux

1	Flux de données sensibles sur le réseau
2	SSL Pinning
3	Contrôles sur la validité des certificats

2.4. Analyse forensique

1	Traces laissé par l'application une fois désinstallée

3. METHODOLOGIE APPLICATION SERVEUR

L'application serveur a profité d'une analyse incluant notamment l'ensemble des vulnérabilités du Top 10 OWASP (www.owasp.org), sans que l'une de celles-ci n'ait été découverte ou soit restée sans correction suffisante.

Tests
Test 1 : Entropie des Cookies
Test 2 : Option de sécurité des Cookies
Test 3 : Cross Site-Scripting
Test 4 : Fixation de session
Test 5 : CRLF injection
Test 6 : Cross Site Request Forgery - CSRF
Test 7 : Protection des communications
Test 8 : Protections anti brute force
Test 9 : Exploration des répertoires
Test 10 : Enumération des utilisateurs

Test 11 : Déni d'accès
Test 12 : Politique de définition de mot de passe
Test 13 : Divulgation d'informations techniques
Test 14 : Injection SQL
Test 15 : Upload de fichiers
Test 16 : Cross Site-Flashing
Test 17 : Référence direct non sécurisé à un objet
Test 18 : Mise à jour des systèmes clés
Test 19 : Sécurité des entêtes HTTP

4. APPRECIATIONS

Dans la mesure où l'application permet d'ouvrir des accès physiques, la sensibilité est de facto élevée. Phonesec teste de nombreuses applications mobiles et applications serveurs dont le niveau de sécurité requis est élevé, dans le même secteur d'activité ou pour des secteurs d'activités comparables.

Les 3 applications testées présentent des garanties de sécurité qui les situent dans la frange haute des applications en matière de protection. L'audit ne révèle pas de faille directement exploitable, ce qui permet de positionner le niveau de sécurité des applications à « haut » pour le domaine d'usage et les exigences de protection.

5. A PROPOS DE PHONESEC

Cette étude a été réalisée par la société PHONESEC pour le compte de STID. PHONESEC est une société française indépendante créée en 2002, labellisée France Cybersecurity. Ses spécialités sont le conseil et l'ingénierie dans la sécurité de l'information ainsi que la lutte contre la fraude dans les nouvelles technologies. Ses références actives sont entre autres les sociétés Allianz, Bouygues Télécom, Gemalto, la GSMA, H3G, Orange Group, Price Minister, Groupe Solimut Mutuelles de France, Caisse d'Epargne, Gendarmerie Nationale, Eurocopter, Samsung, SFR, Alcatel, Vodafone Group, VSC Technologies, CMA CGM, Showroomprivé, Snef, et de nombreuses autres.

PHONESEC
27 boulevard Charles Moretti
13014 Marseille France
Site Internet : http://www.phonesec.com
Email : contact@phonesec.com