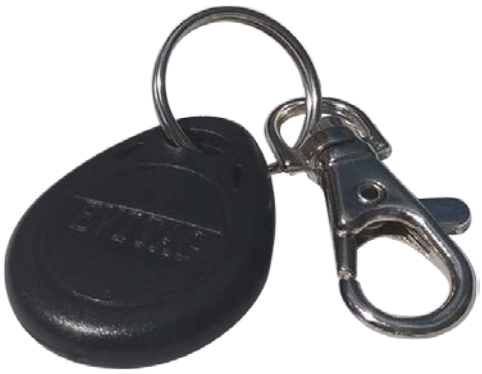

BUG BOUNTY EXPRESS
*Stand **Fullsecure / CONAND 2018***
7-8 Février / ANDORRA

Détails du Bug Bounty Express

Cible

La cible du Bug Bounty Express est détectée des vulnérabilités sur le produit EVITAG NFC. Le produit comprend une application sous Android et un module électronique NFC.

Scénarios

Récupérer les login et mots de passe hébergés à l'intérieur d'un coffre-fort EVITAG NFC

Période

Durée : 2 jours
Horaire : 10h à 18h30
Date : du 7 au 8 février 2018

Lieu

Centre de Congressos d'Andorra la Vella
Plaça del Poble, AD500 Andorra la Vella
(https://goo.gl/maps/VWQGtK2ADkS2)

Evènement

CONAND 2018
https://conand.ad

Accès au Bug Bounty

Gratuit et libre d'accès
Stand Fullsecure « Bug Bounty Express Evitag NFC »
Inscription en ligne : https://wp.me/P72I8X-jE

Freemindtronic SL Andorra
Av. Copríncep de Gaulle, núm. 13
Edifici Valira planta Baixa
AD700 Escaldes – Engordany
NRT : L-711610- PRINCIPAT D'ANDORRA

Matériel mis à disposition

Cinq EVITAG NFC ID5 contenant 5 labels, 5 login & 5 mots de passe, brute force activée avec mot de passe administrateur et jamming activé.
Un EVITAG NFC ID5 contenant 5 labels, 5 login & 5 mots de passe, brute force activée et jamming activé, dédié aux l'attaques brute force physique (Tamper-proof)

Seront disponibles 5 postes.
Chaque poste est composé de :

- 1 EVITAG NFC ID5
- Tables
- Chaises
- Connexion internet
- Multi prise électrique
- 1 Oscilloscope 4 voies
- 1 Capteur thermique professionnel (Etalonné) avec capture d'image thermique
- 1 Routeur WIFI création d'un réseau local pour la fonction de EVILOCK NFC

Matériel du participant

Le participant doit posséder au minimum un smartphone sous Android disposant de la technologie NFC.

Le participant est libre d'utiliser tout type de matériel pour réaliser ses attaques.

Le participant apporte son matériel sous son unique responsabilité, tel qu'ordinateur, smartphone, appareils de mesure et/ou radio fréquence.

Pour les attaques brute force physique, le participant apporte son outillage et /ou des solutions d'attaques physiques. Entendu, que les outils et/ou solutions pouvant porter atteinte à l'intégrité des personnes physiques est prohibé dans le cadre de l'évènement CONAND. Dans l'hypothèse où le participant souhaite réaliser ce type de test, il devra en faire la demande explicite et motivée. La demande acceptée par Fullsecure, devra être réalisée en dehors du cadre de l'événement à l'extérieur dans un environnement sécurisé par le participant. Au moins un témoin sera présent lors de l'attaque physique et sera filmé par une personne de l'entreprise Fullsecure.

Contrainte des attaques

D'une manière générale toute les attaques brute force sont autorisées, qu'elles soient passives et/ou intrusives. On considère les attaques :

- numérique
- électronique
- radio fréquence
- physique (les attaques physiques (sur le Tamper-proof d'EVITAG NFC) doivent faire l'objet d'une demande préalable à Fullsecure lors de l'événement. En effet une attaque physique peut endommager de manière irrémédiable l'intégrité de fonctionnement de l'EVITAG NFC. Il sera demandé au participant de motiver le type d'attaque physique qu'il souhaite réaliser avant de percevoir un EVITAG NFC. Entendu, qu'aucun EVITAG NFC ne sera donné pour le même type d'attaque visant à détruire l'enveloppe plastique ou la matière solide qui enrobe la carte électronique)..
- Root du smartphone
- Attention l'utilisation du WIFI en Réseau local du centre des congrès d'Andorre ne permet pas d'utiliser la fonction EVILOCK NFC. Vous devrez utiliser un réseau local dédié pour le Bug Bounty avec accès à internet.

Récompenses

Seule la capture des libellés présents dans les cinq EVITAG NFC ID5 non chiffré sont éligible pour la récompense. Voir ci-dessous pour plus de détails.

Cibles	Récompense
Gravité légère : Le participant a détecté un problème de sécurité suffisamment critique qui impliquera une modification du code à court terme.	1 x DUO EVITAG 115
Gravité intermédiaire Tamper-Proof : Le participant réussit à forcer le Tamper Proof du module EVITAG NFC de manière intrusif ou non intrusif et toujours 100% fonctionnel. Le participant a accès à la carte électronique et ses composants.	1 x DUO EVITAG 115
Gravité moyenne : Le participant a réussi à capturer la clé appairage de l'EVITAG NFC	1 x DUO EVITAG 115 Une nuit à l'hôtel GOLDEN TULIP d'Escaldes-Engordany EN PENSION COMPLETE POUR 2 PERSONNES
Gravité sévère : Le participant a réussi à tous capturer la clé d'appairage + le mot de passe administrateur + les login & mots de passe hébergés dans la mémoire	1 x DUO EVITAG 115 Une nuit à l'hôtel GOLDEN TULIP d'Escaldes-Engordany EN PENSION COMPLETE POUR 2 PERSONNES Entrée Inúu + soin 30' + Private Wellness Spa à CALDEA pour 2 personnes

Certification des résultats

Les identifiants (clés d'appairage, labels et mots de passe présents dans les six EVITAG NFC) sont remis aux organisateurs de CONAND sous enveloppe cachetée.

Il est précisé que les clés d'appairage, les mots de passe adminitrateur, les labels, les login et les mots de passe sont uniques.

Fullsecure a en sa possession la copie exacte du document cacheté fourni à l'organisateur de l'événement CONAND.

Authentification

La réussite du participant est considérée comme authentification dans la mesure où le participant est en mesure de réaliser la démonstration explicite de son attaque qui lui a permis de récupérer tout ou partie des données hébergées dans l'EVITAG NFC. Les clés d'appairage et/ou les labels et/ou les mots de passe récupérés doivent être identiques au document de certification présenté par Fullsecure. En cas de conteste, le participant peut demander la confirmation par l'enveloppe cachetée remise à l'organisateur.

Identité du participant

L'identité des participants doit être préalablement connue de Fullsecure. Les informations suivantes seront demandées :

- Etat civil
- Adresse
- Profession
- Entreprise (facultatif)
- Mail
- Tel (facultatif)

Entendu, que toutes ces informations demeureront confidentielles pour l'entreprise Fullsecure. Elles ne seront utilisées qu'à des fins de traçabilité à usage interne et statistiques.

Deux possibilités pour l'inscription des participants :

L'inscription peut être réalisée sur le lieu et pendant l'évènement en remplissant un document de renseignement et d'acceptation du règlement des conditions de participation.

Le participant s'inscrit sur le site internet à l'adresse suivante : https://wp.me/P72I8X-jE

Domaines de concentration:

- Récupérer la clé d'appairage en clair
- Récupérer le mot de passe administrateur en clair
- Récupérer les logins hébergés dans EVITAG NFC en clair
- Récupérer les mots de passe hébergés dans EVITAG NFC en clair
- Récupérer le code du brouillage d'affichage
- Connexion automatique en LAN via réseau local dédié « Bug Bounty Conand »

Exclusions générales soumises à autorisation :

Afin de respecter les règles de sécurité du Centre du Congrès d'Andorre.

- Attaques DDoS / DoS
- Les attaques d'énumération nécessitent une notification et une approbation préalables

Bugs exclus pour l'application Android

- Dans le principe rien n'est exclus, y compris les débogueurs numérique et/ou matériel et/ou autres outils.
- Cependant, seuls les bugs critiques permettant d'accéder aux données (mot de passe administrateur, clé appairage, login et mot de passe) seront retenus pour valider la réussite de la cible du Bug Bounty.

Bugs exclus pour les autres systèmes d'exploitation

Dans le principe, le participant utilise son matériel, il est donc l'unique responsable de son usage. Le seul élément sous la responsabilité de Fullsecure est l'application « EVITAG NFC » publiée et disponible gratuitement sur Google Play :

https://play.google.com/store/apps/details?id=com.freemindtronic.evitagnfc

FULLSECURE peut veut vous aider !

Si vous souhaitez obtenir des informations sur l'application, ou si vous avez des questions concernant l'application qui pourraient vous aider, veuillez créer une soumission et demander cette information.

A noter que l'application possède une notice d'utilisation disponible sur YouTube :

Play liste : **EVITAG NFC**

https://www.youtube.com/playlist?list=PLLyNxN21uUIpyflF19qN-zIGGTzTUibM3

Play liste : **EVILOCK NFC**

https://www.youtube.com/playlist?list=PLLyNxN21uUIptcTAqFrw6yxXvmdOVrwkZ

Animateur poste Bug Bounty

Un animateur sera présent pour répondre aux diverses questions des participants.

Le participant peut aussi envoyer un mail à l'adresse suivant :

bugbounty2018@fullsecure.link

Si vous avez des questions concernant le fonctionnement de l'application, ou des demandes d'informations sur l'Application Android vous êtes encouragés à les envoyer par courriel à bugbounty2018@fullsecure.link

Fullsecure acceptera également les soumissions d'hypothèses fautives, sans pénalité, et travaillera avec le participant pour développer une hypothèse raisonnable dans un exploit opérationnel, si cela est possible.

Notes sur le produit

EVITAG NFC est un module endurci faisant office de coffre-fort physique, qui héberge des labels composés en principe de login et mot de passe permettant par exemple la connexion automatique aux comptes sur internet.

Il fonctionne uniquement via le NFC d'un smartphone utilisé comme terminal préalablement appairé avec une clé unique. Il héberge les données de manière chiffrée en AES256 dans une mémoire non volatile physiquement sécurisée.

Le module EVITAG NFC est tamper proof et dépourvu de batterie. Il produit sa propre énergie pour fonctionner. Toutes les données qu'il héberge sont physiquement sauvegardées et sont toujours disponibles, pendant une durée d'au moins quarante sans être utilisées.

EVITAG NFC fonctionne en temps réel avec les mémoires électroniques dédiées internes. La technologie brevetée n'utilise aucune base de données, ni de connexion internet pour héberger et gérer les données.

Il dispose d'une fonction administrateur et utilisateur qui verrouille l'utilisation de fonction critique. Ce système permet d'utiliser un EVITAG NFC sans avoir besoin de connaître le mot de passe pour vous connecter à un compte sur internet.

Avec EVITAG NFC vous êtes mobile, furtif, ne laisser aucune trace numérique et vous pouvez vous connecter sur n'importe quel ordinateur.

L'application EVITAG NFC ainsi que le plugin EVILOCK NFC sont gratuits et libres de tout engagement financier. Non intrusif, le module fonctionne avec le plugin EVILOCK NFC disponible comme extension pour Chrome et Mozilla, qui permet de gérer des flottes de smartphone et d'EVITAG NFC pour se connecter aux comptes sur internet sans avoir besoin de connaître et visualiser le mot de passe.

EVITAG NFC est la seule application au monde capable de partager en clair son mot de passe de manière sécurisée grâce à la fonction « jamming ». Envoyer un mot de passe à une personne est aujourd'hui possible en toute sécurité via n'importe quel service de messagerie chiffrée ou en clair.

Le module est discret, se confond avec un tag RFID. Il est waterproof, endurci à l'extrême et fonctionne à des températures extrêmes de -40 à +85°.

Pour plus d'informations, vous pouvez visiter le site EVITAG NFC. Des informations supplémentaires peuvent être trouvées ici.

Règles

Ce scénario est encadré par des règles de confidentialité de non divulgation d'éventuels bugs découverts lors de l'événement. Entendu, que la divulgation de l'identité du participant à l'origine de la découverte est soumise à sa demande préalable selon les « Conditions standard de divulgation Bug Bounty de Fullsecure®».

Ce programme n'offre pas de récompenses pour les résultats déjà connus et publiés dans les notes de version.

Il est entendu que la divulgation et la communication des informations qui ont conduit à la récompense sont soumis à une autorisation préalable et explicite de fullsecure®.

Droit à l'image

Le scénario du Bug Bounty est réalisé dans un lieu ouvert au public. Des photographies peuvent être prises des participants. En conséquence de quoi et conformément aux dispositions relatives au droit à l'image, le participant autorise à fixer, reproduire et communiquer au public les photographies prises dans le cadre du Bug Bounty EVITAG NFC à Conand 2018.

Il est entendu, que les photographies pourront être exploitées et utilisées directement par Fullsecure®, sous toute forme et tous supports connus et inconnus à ce jour, dans le monde entier, sans limitation de durée, intégralement ou par extraits et notamment : - Presse, - Livre, - Carte postale, - Exposition, - Publicité, - Projection publique, - Concours, - Autre. Fullsecure®, s'interdit expressément de procéder à une exploitation des photographies susceptible de porter atteinte à la vie privée ou à la réputation, et d'utiliser les photographies de la présente, dans tout support à caractère pornographique, raciste, xénophobe ou toute autre exploitation préjudiciable.

Le participant reconnaît être entièrement rempli de ses droits et ne pourra pas prétendre à une rémunération pour l'exploitation des droits. Le participant garantis qu'il n'est pas lié par un contrat exclusif relatif à l'utilisation de son image ou de son nom. Il explicitement établit que tout litige né de l'interprétation ou de l'exécution des présentes, il sera fait attribution expresse de juridiction des tribunaux Andorran en langue Catalane.