BUG BOUNTY EXPRESS

*Stand **Fullsecure / CONAND 2018***
7-8 Février / ANDORRA

Details of the Bug Bounty Express

Cible

The target of the Bug Bounty Express is detected on the EVITAG NFC product vulnerabilities. The product includes an application on Android and an NFC electronic module.

Scenaris

Recover login and password hosted inside an EVITAG NFC safe

Period

Duration : 2 days

Time : 10am to 6.30 pm

Date : 7 and 8 february 2018

Place

Centre de Congressos d'Andorra la Vella

Plaça del Poble, AD500 Andorra la Vella

https://goo.gl/maps/VWQGtK2ADkS2

Event

CONAND 2018
https://conand.ad

Access to the Bug Bounty

free and free of access
Stand of Bug Bounty « expositor place »
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

Material available

Five EVITAG NFC ID5 containing 5 labels, 5 login & 5 passwords, protection brute force ON with password admin and jamming ON
An EVITAG NFC ID5 containing 5 labels, 5 login & 5 passwords, protection brute force ON with password admin and jamming ON dedicated to brute force attack (under conditions)

Will be available 5 positions.
Each position is composed of:

- 1 EVITAG NFC ID5
- Tables
- Chairs
- Internet connection
- Electrical power strip
- 1 4-channel oscilloscope
- 1 Professional thermal sensor (Calibrated) with thermal image capture
- 1 WIFI router creating a local network for EVILOCK NFC function

Material of the participant

The participant must have at least one Android smartphone with NFC technology.

The participant is free to use any type of material to carry out his attacks.

The participant brings his equipment under his sole responsibility, such as computer, smartphone, measuring devices and / or radio frequency.

For brute-force brute force attacks, the participant brings his or her tooling and / or physical attack solutions. That tools and / or solutions that could affect the integrity of individuals is prohibited in the context of the event CONAND. In the event that the participant wishes to carry out this type of test, he will have to make the explicit and motivated request. The request accepted by Fullsecure, must be carried out outside the framework of the event outside in a secure environment by the participant. At least one witness will be present during the physical attack and will be filmed by someone from Fullsecure.

Stress of attacks

In general, all brute force attacks are allowed, whether passive and / or intrusive. We consider the attacks:

- Digital
- electronic
- radio frequency
- Physical (Physical attacks must be requested by Fullsecure at the time of the event, as a physical attack may irreparably damage the operating integrity of the EVITAG NFC. to motivate the type of physical attack he / she wishes to perform before receiving an NFC EVITAG.However, that no NFC EVITAG will be given for the same type of attack aimed at destroying the plastic wrap or the solid material that coats the electronic card).
- Root of the smartphone
- Attention the use of WIFI in local network of the congress center of Andorra does not allow to use the function EVILOCK NFC. You will need to use a dedicated local network for the Bug Bounty with internet access.

Adwards

Only the capture of the clear data present in the five EVITAG NFC ID5 is eligible for the award. See below for more details.

Cibles	Adwards
Slight Gravity: The participant has detected a sufficiently critical security issue that will imply a short-term code change.	1 x DUO EVITAG NFC 115
Intermediate gravity Tamper-Proof: the participant managed to force the Tamper Proof of functional module EVITAG NFC in intrusive or non-intrusive manner and always 100%. The participant has access to the electronic map and its components.	1 x DUO EVITAG NFC 115
Mean Severity: The participant was able to capture the pairing key of the EVITAG NFC	1 x DUO EVITAG NFC 115 One night at the hotel GOLDEN TULIP in Escaldes-Engordany fullboard ofr 2 people
Severe severity: The participant was able to capture the pairing key + the administrator password + the login & passwords stored in the memory.	1 x DUO EVITAG NFC 115 One night at the hotel GOLDEN TULIP in Escaldes-Engordany fullboard ofr 2 people One admission Inúu + care 30' + Private Wellness Spa at CALDEA for 2 people

Certification of results

The identifiers (pairing keys, labels and passwords present in the six NFC EVITAG) are given to the CONAND organizers in a sealed envelope.

It is specified that the pairing keys, the admin passwords, the labels, the login and the passwords are unique.

Fullsecure has in its possession the exact copy of the sealed document provided to the organizer of the CONAND event.

Authentication

The success of the participant is considered as authentication to the extent that the participant is able to perform the explicit demonstration of his attack that allowed him to recover all or part of the data hosted in the EVITAG NFC. The pairing keys and / or labels and / or passwords recovered must be identical to the certification document presented by Fullsecure. In case of dispute, the participant may request confirmation by the sealed envelope given to the organizer.

Identity of the participant

The identity of the participants must be previously known to Fullsecure. The following information will be requested:

- Full civil status
- Address
- Profession
- Company (optional)
- Mail
- Tel (optional)

We understand that all this information will remain confidential for Fullsecure. They will only be used for traceability purposes for internal use and statistics.

Two possibilities for registering participants:

- Registration can be done at the venue and during the event by completing an information document and acceptance of the rules of participation.
- The participant registers on the website at the following address: https://wp.me/P72I8X-jE

Domains of concentration:

- Get the pairing key in clear
- Retrieve the administrator password in clear
- Retrieve hosted logins in EVITAG NFC unencrypted
- Recover passwords hosted in EVITAG NFC unencrypted
- Retrieve display scrambling code
- Automatic LAN connection via dedicated local network "Bug Bounty Conand"

General exclusions subject to authorization:

In order to respect the safety regulations of the Congress Center of Andorra.

- DDoS / DoS attacks
- Enumeration attacks require prior notification and approval

Excluded bugs for the Android app

- In principle nothing is excluded, including digital and / or hardware debuggers and / or other tools.
- However, only the critical bugs allowing access to the data (administrator password, key pairing, login and password) will be retained to validate the success of the Bug Bounty target.

Excluded Bugs for the others operating systems

In principle, the participant uses his equipment, so he is solely responsible for its use. The only item under the responsibility of Fullsecure is the "EVITAG NFC" app published and freely available on Google Play.

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

FULLSECURE can help you!

If you would like information about the app, or if you have any questions about the app that might help you, please create a quote and request that information.

Note that the application has a user manual available on 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

A facilitator will be present to answer the various questions of the participants.
The participant can also send an email to the following address: bugbounty2018@fullsecure.link

If you have any questions about the operation of the app, or requests for information about the Android App you are encouraged to email them to bugbounty2018@fullsecure.link

Fullsecure will also accept submissions of faulty assumptions, without penalty, and will work with the participant to develop a reasonable assumption in an operational exploit, if at all possible.

Device's notes :

EVITAG NFC is a hardened module acting as a physical safe, which hosts labels composed in principle of login and password allowing for example the automatic connection to accounts on the internet.

It only works via the NFC of a smartphone used as a previously paired terminal with a unique key. It hosts the data encrypted in AES256 in a physically secure non-volatile memory.

The EVITAG NFC module is tamper proof and battery-free. It produces its own energy to work. All the data it hosts is physically saved and is always available, for a period of at least forty without being used.

EVITAG NFC works in real time with internal dedicated electronic memories. The patented technology does not use any database or internet connection to host and manage data.

It has an administrator and user function that locks the use of critical function. This system allows you to use an EVITAG NFC without needing to know the password to connect to an account on the internet.

With EVITAG NFC you are mobile, stealthy, leave no digital traces and you can connect to any computer.

The EVITAG NFC application and the EVILOCK NFC plugin are free and free of any financial commitment. Non-intrusive, the module works with the EVILOCK NFC plugin available as an extension for Chrome and Mozilla, which allows to manage fleets of smartphone and EVITAG NFC to connect to the accounts on the internet without needing to know and view the password.

EVITAG NFC is the only application in the world able to share its password in a secure way thanks to the "jamming" function. It is now safe to send a password to any person via any encrypted or unencrypted e-mail service.

The module is discrete, merges with an RFID tag. It is waterproof, hardened to the extreme and operates at extreme temperatures from -40 to + 85 °.

For more information, visit the EVITAG NFC website. Additional information can be found here.

Rules

This scenario is framed by confidentiality rules of non-disclosure of any bugs discovered during the event. Understood, that the disclosure of the identity of the participant at the origin of the discovery is subject to its prior request according to the "Standard Terms of Disclosure Bug Bounty of Fullsecure®".

This program does not offer rewards for results already known and published in the release notes.

It is understood that the disclosure and disclosure of the information that led to the award is subject to prior and explicit authorization from fullsecure®.

Right to the image

The scenario of the Bug Bounty is made in a place open to the public. Photographs can be taken of the participants. As a result of and in accordance with the provisions relating to the right to the image, the participant authorizes to fix, reproduce and communicate to the public the photographs taken under the Bug Bounty EVITAG NFC in Conand 2018.

It is understood, that the photographs will be able to to be exploited and used directly by Fullsecure®, in any form and medium known and unknown to date, throughout the world, without limitation of duration, in full or by extracts and in particular: - Press, - Book, - Postcard, - Exhibition, - Advertising, - Public screening, - Contests, - Other. Fullsecure® expressly prohibits the exploitation of photographs that may infringe privacy or reputation, and use the photographs herein, in any pornographic, racist, xenophobic or other media detrimental exploitation.

The participant acknowledges that he is completely full of his rights and can not claim remuneration for the exploitation of the rights. The participant guarantees that he is not bound by an exclusive contract relating to the use of his image or his name. It explicitly establishes that any dispute arising from the interpretation or execution of the present, will be made express jurisdiction of the Andorran courts in Catalan language.