Security Advisory

SAS Scandinavian Airlines v1.0 for iOS: Multiple vulnerabilities

13th of May 2013

Juan J. Güelfo
CEO, IT-security consultant and
IT-security researcher at Encripto AS

About Encripto AS

Encripto AS is a Norwegian company which provides specialized services in IT-security with superior quality. Our core expertise is education, security testing and security monitoring.

Encripto AS is committed to information security. We do research to discover trends, new vulnerabilities and better ways to mitigate them. We believe in acting as good internet citizens to the industry, whether you are a provider or a user.

You can read more about us at http://www.encripto.no

Timeline and revision history

- ***13th of May 2013***
  Public release of the security advisory.

- ***10th of May 2013***
  Scandinavian Airlines informs Encripto AS that a new version of the mobile application has been released, and that the security issues have been solved.

- ***8th of May 2013***
  Scandinavian Airlines releases SAS Scandinavian Airlines v1.0.1 with bug fixes.

- ***29th of April 2013***
  Initial version (non-public disclosure). Encripto AS contacts Scandinavian Airlines (SAS) and sends a copy of the advisory.

- ***26th of April 2013***
  Vulnerabilities are discovered by the researcher.

Disclaimer

The material presented in this document is for educational purposes only. Encripto AS cannot be responsible for any loss or damage carried out by any technique presented in this material. The reader is the only one responsible for applying this knowledge, which is at his / her own risk.

No servers, external clients or individuals were breached during this research. The vulnerabilities were found using the researcher's mobile device.

Any of the trademarks, service marks, collective marks, design rights, personality rights or similar rights that are mentioned, used or cited in this document is property of their respective owners.

License

1. Background

SAS Scandinavian Airlines for iOS is a personal in-phone travel agent. It gives EuroBonus members the opportunity to book SAS tickets, check in, access boarding passes and manage flights.

The app also allows new users to register and become EuroBonus members.

Please visit iTunes for more information about the app:
https://itunes.apple.com/no/app/sas-scandinavian-airlines/id605727126?mt=8

2. Description

Encripto AS has discovered multiple vulnerabilities in SAS Scandinavian Airlines (v1.0) for iOS.

The vulnerabilities could allow an attacker to take control over EuroBonus member's accounts (adjacent network attack vector) and / or steal credit card information (local attack vector).

3. Affected software

SAS Scandinavian Airlines v1.0 for iOS. Other platforms may be also vulnerable.

4. Vulnerabilities

The list below describes the vulnerabilities discovered in the affected software.

- **App vulnerable to Man-In-The-Middle attacks**
  The mobile application is vulnerable to Man-In-The-Middle (MITM) attacks. The application does not validate the server SSL/TLS certificate in a proper way. The issue occurs before establishing a secure connection with the server during the login process.

  As a result, the attacker can get access to the user information sent by the mobile device, including username and password.

  Proof of Concept
  The request below is an example of what the attacker would capture (parameters have been anonymized):

```
POST /mobilegw/latest/sso/login HTTP/1.1
Host: gui.flysas.net
Proxy-Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept-Language: en-us
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Origin: null
Cookie: strSec=3; PHPSESSID=ab6a31da00ffed51ea4e1291cb7e74d1
Content-Length: 124
Connection: keep-alive
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 6_1_3 like Mac OS X)
AppleWebKit/536.26 (KHTML, like Gecko) Mobile

token=14b7f00fc54c819f53e099565aaaa03e&sig=a2f9ae948393f32c5ba0c5e765e6013bcaf
945c5&userName=600601602&password=Password123
```

- ***Credit card information stored in clear text***
  The mobile application keeps a local cache which stores the URLs visited by the application. These URLs are saved with parameter data.

  If the user submits a payment when booking a flight, or decides to store a credit card in the system, the mobile application will transmit the transaction information via GET requests. In other words, the information will be transmitted via URL parameters.

  The transactions will be stored in the application's local cache completely unencrypted:

  - **Database file:** ./Library/Caches/sas.se.sascore/Cache.db
  - **Table:** cfurl_cache_response
  - **Column:** request_key

  Proof of Concept
  The next two examples illustrate the vulnerability (parameters have been anonymized):

```
http://book.flysas.com/SAS/dyn/air/booking/book;jsessionid=<sessionID>SITE=SKA
ASKAA&LANGUAGE=GB&PAGE_TICKET=3&PAYMENT_TYPE=CC&DELIVERY_TYPE=ETCKT&ACTION=BOO
K&WDS_TRAVELLERS_IDS=1&AIR_CC_ADDRESS_ID=AIR_1&EMAIL_FOOTER_CONTENT=&SLIDER_CA
SH=3728.00&SLIDER_MILES=0&WDS_SLIDER_VALUE=0&terms=on&CC_ID=CC_1&WDS_CC_TYPE=V
I&WDS_CC_NUMBER=4925000000000004&CC_DIGIT_CODE_1=123&CC_EXP_1=06%2F13&CC_DESCR
IPTION_1=Test1&CC_NAME_ON_CARD_1=Navn+Navnesen&CC_NUMBER_1=4925000000000004&CC
_TYPE_1=VI&CC_TOBE_STORED_1=TRUE&CC_TOBE_DEFAULT_1=FALSE
```

```
http://book.flysas.com/SAS/dyn/air/profile/updateCreditCards;jsessionid=<sessi
onID>USER_ID=&SITE=SKBKSKBK&LANGUAGE=GB&CC_ID=CC_1&CC_TOBE_DELETED_1=FALSE&CC_
EXP_1=05%2F13&CC_ACTION_1=insert&ORIGIN_PAGE_1=profilePage&CC_DESCRIPTION_1=Te
st1&PRESELECTED=&CC_NAME_ON_CARD_1=+Navn+Navnesen&CC_TYPE_1=VI&CC_DISPLAY_NUMB
ER_1=4925000000000004&CC_NUMBER_1=4925000000000004&month_1=05&year_1=13&CC_TOB
E_STORED_1=TRUE&CC_ID_1=Test1&CC_TOBE_DEFAULT_1=FALSE&WDS_DEF_CC=CC_1
```

- ***User registration transmitted via HTTP***
  The mobile application gives the possibility to register new users. The system will require personal information, such as e-mail address, username, password, mobile phone number, first name, last name, date of birth, gender, address, postal code, city and country.

  The user registration is handled via HTTP (unencrypted protocol), which can be easily intercepted.

  Proof of Concept
  The request below is sent by the mobile application during a user registration (parameters have been anonymized):

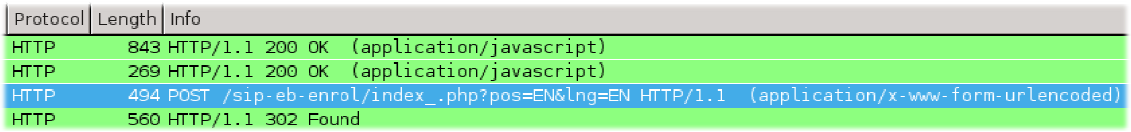

Fig. 1: HTTP traffic sent by the mobile application during user registration

```
POST /sip-eb-enrol/index_.php?pos=EN&lng=EN HTTP/1.1
Host: gui.flysas.net
Referer: http://gui.flysas.net/sip-eb-
enrol/mobile/?lng=EN&pos=EN&mode=ios&udid=8128175576611648879&hidden_campaign_
code=mobileapp&utm_source=mobileapp
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content-Type: application/x-www-form-urlencoded
Accept-Language: nb-no
Accept-Encoding: gzip, deflate
Origin: http://gui.flysas.net
Cookie: strSec=3; PHPSESSID=ab6a31da00ffed51ea4e1291cb7e74d1
Content-Length: 408
Connection: keep-alive
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 6_1_3 like Mac OS X)
AppleWebKit/536.26 (KHTML, like Gecko) Mobile

pos=EN&lng=EN&ts=&mode=ios&domain=&hidden_campaign_code=mobileapp&popupconf=&m
obile=2&channel=app&debug=0&udid=8128175576611648879&view=ios&email=test%40exa
mple.com&username=test%40example.com&password=Password123&mobilephone=%2B47222
11333&mobilephone%2B=&firstname=Navn&lastname=Navnesen&birthdate=1960-04-
01&gender=M&addressLine1=Testgate&postcode=5000&city=Teststad&country_lng=FI&c
ountry=NO&confirm_rules=on
```

5. Solution

Users should update their app to version 1.0.1.

6. Credit

The vulnerabilities were discovered by Juan J. Güelfo, at Encripto AS.
E-mail: post@encripto.no
Web: http://www.encripto.no

For more information about our research policy, please visit http://www.encripto.no/forskning/