# IOActive Security Advisory

| Title | Facebook Access Token Sent in Plaintext |
|---|---|
| Severity | High |
| Discovered by | Ariel M. Sanchez |

## Affected Products

Version: Instagram 5.0.3

Tested on: iPhone iOS 7.0.4

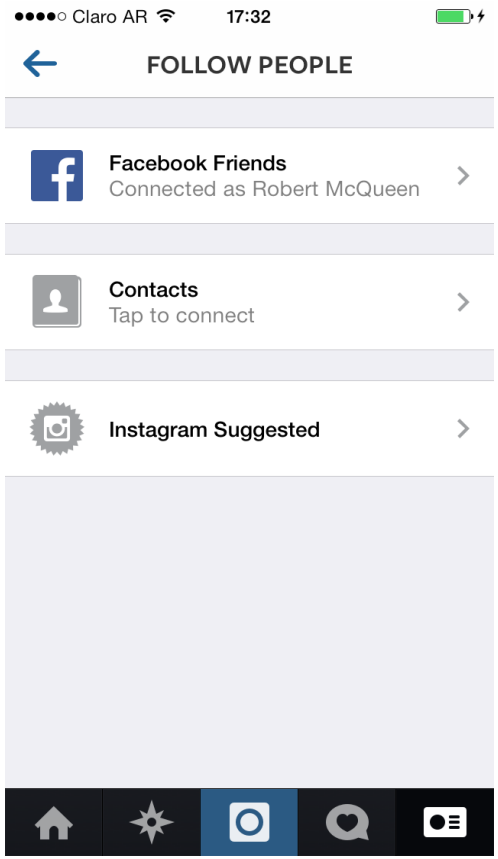
## Impact

Attackers can steal Facebook access tokens to impersonate victim Facebook users and perform malicious actions that include, but are not limited to, posting content on behalf of users and accessing friend lists.

*Copyright ©2014. All Rights Reserved. [1]*

## Technical Details

When an Instagram user selects the Facebook “Friends” functionality, the Facebook access token is embedded in the POST body and sent to the web server in plaintext through HTTP. Attackers can gain access to the token by sniffing network traffic:




*Copyright ©2014. All Rights Reserved. [2]*

## Proof of Concept

The Facebook Friends functionality performed this request to validate the Facebook access token:

```
POST /api/v1/fb/find/?include=extra_display_name HTTP/1.1
Host: instagram.com
Proxy-Connection: keep-alive
Accept: */*
Accept-Encoding: gzip, deflate
Content-Length: 337
Content-Type: multipart/form-data; boundary=Boundary+0xAbCdEfGbOuNdArY
Accept-Language: en;q=1, es-MX;q=0.9, fr;q=0.8, de;q=0.7, zh-Hans;q=0.6, zh-Hant;q=0.5
Cookie: ccode=AR; csrftoken=dab2c8d0c4fd28627ac9f2a77fa221d2; ds_user_id=1045525821;
igfl=testlocura; is_starred_enabled=yes; mid=UuvAbgAAAAHj6L0tnOod5roiGYnr;
sessionid=IGSC3aaf1427aa901bb052263b368642a34fe59897cba046682b7d95775ae70db64d%3AioaQSiHdJ61kCj
uRaAD9sEJTEWXv6dqB%3A%7B%22_token%22%3A%221045525821%3Au91J1dZgsiJCBo0QVeF98nkohO0TV928%3A70d9e
ee5449941dc80fb238991e191f8f33cac5c98c1b078d86975b07979531d%22%2C%22last_refreshed%22%3A1392496
331.661547%2C%22_auth_user_id%22%3A1045525821%2C%22_auth_user_backend%22%3A%22accounts.backends
.CaseInsensitiveModelBackend%22%2C%22_platform%22%3A0%7D
Connection: keep-alive
User-Agent: Instagram 5.0.2 (iPhone5,3; iPhone OS 7_0_4; en_US; en) AppleWebKit/420+

--Boundary+0xAbCdEfGbOuNdArY
Content-Disposition: form-data; name="fb_access_token"

CAABwzLixnjYBAE71ZAmnpZAaJeTcSqnPSSvjEZA0CqIokUOj60VkZCOhuZCy4dT6TlcG9OpbMIO7dJnGiROm7XFEnRj...
.
--Boundary+0xAbCdEfGbOuNdArY--
```

*Copyright ©2014. All Rights Reserved. [3]*

The affected token received these Facebook permissions:

- installed
- basic_info
- public_profile
- create_note
- photo_upload
- publish_actions
- publish_checkins,
- publish_stream
- status_update
- share_item
- video_upload
- user_friends

### Solution

This issue is fixed. Upgrade to Instagram version 6.0.4 or later.

*Copyright ©2014. All Rights Reserved. [4]*