Instagram Photo Upload and Flattr Money Redirection Vulnerability

Affected app: Instagram (Android/iOS)

Affected versions: 4.0.2, 4.1.2 and 4.2.7, probably also earlier versions affected.

Summary

Last year and earlier this year some vulnerabilities in Instagram (Android/iOS) were discovered, which give an attacker the ability to like and delete photos in the name of the hijacked account. Accounts can be hijacked based on plaintext communication of the Instagram app, i.e. in unencrypted WiFi networks.

We discovered two new security flaws in Instagram.

With these vulnerabilities Mallory is able to upload photos into Alice's account and, much more significant, steal money if Alice linked her Instagram account to Flattr. Normally this feature provides the ability for Alice to flattr the photos she "likes". The fact that Mallory can "like" photos in Alice's name gives her the ability to flattr content in the name of Alice. Mallory can now create her own Instagram account, link it with her Flattr, upload random photos and flattr these photos with Alice's Instagram account to get money from her.

Photo upload

The photo upload in Instagram happens in two steps. In the first step the photo is sent via **unencrypted** HTTP with a POST request to `/api/v1/media/upload/`, which returns a media_id.

In the second step, an activation request is sent over HTTPS to `/api/v1/media/configure`. We analyzed this request using a MitM attack. With a custom SSL Root CA certificate installed on our Android and iOS devices, we were able to redirect the SSL secured traffic to Instagram to obtain the plain text of the requests:

```
POST /api/v1/media/configure/ HTTP/1.1
Host: instagram.com
[more headers stripped]

signed_body=eb8b5bdff7bf8ba402a50c69617a50a23e49367ff3d470dd447f658d64a95c25.{"filter_type":28,"med
ia_id":"593984755223468908_68...","device_timestamp":1384857213,"caption":"example","_uuid":"C94EB9
B6...","_uid":"686...","_csrftoken":"0df2b022...","geotag_enabled":false,"usertags":"{\"in\":[]}","
source_type":1,"faces_detected":0}
```

In the body of that request a JSON table is sent to the Instagram server to activate the uploaded photo. The `signed_body` consists of the JSON string and a signature, generated with a hard coded encryption key found in the Instgram app binary. Even though the app uses HTTPS, the same operation can be performed via unencrypted HTTP.

While testing the MitM attack we determined that the Instagram app checks for valid SSL certificates and doesn't send any encrypted requests. This check is sufficient in most cases, however we suggest to additionally perform certificate pinning to further increase security of user data.

Flattr connection

Flattr implemented the ability to link an Instagram account with a Flattr account. If the accounts are linked, by default photos will be automatically flattred whenever a photo is “like”d on Instagram.

Because we are able to like photos by hijacking accounts, we are able to flattr photos in the name of the hijacked user. This requires that a user has linked their Instagram and Flattr accounts.

The “like” request is sent over HTTP and looks as follows:

```
POST /api/v1/media/5762384562834658345 7_8349573845/like/?d=0&src=timeline&ig_sig_key_version=4
Host: instagram.com
[more headers stripped]

signed_body=975428627f0636623d48bc7e88573a8ce05398311738e19469c343cc60b0e78b.{"_uid":"83854...","_c
srftoken":"0df2b022...","media_id":"5762384562834658345 7_8349573845"}
```

Because we know the media ids of our own photos, we can “like” them with the hijacked account and money starts rolling in.

Mitigation

To prevent this attack happening to you, do not use the Instagram app in any network you do not trust completely, i.e. free WiFi hotspots. Instead, only use the app via VPN connections to a trusted site.

To prevent losing money when somebody hijacks your Instagram account, disable the account link on Flattr, or at least disable automatic flattring of photos.

Hijacked flattrs can be seen on the users Flattr notifications dashboard.

Timeline

- 2013–07–21 Signature faking vulnerability discovered.
- 2013–07–23 The vendor was contacted via e-mail, there was no reply yet.
- 2013–08–26 Publication of the signature faking vulnerability.
- 2013–10–14 Photo upload vulnerability discovered.
- 2013–11–18 Flattr money redirection vulnerability discovered.
- 2013–11–21 Publication of the photo upload and flattr vulnerabilities.

Resources

- Instagram 3.1.2 For iOS, Plaintext Media Information Disclosure Security Issue (Carlos Reventlov)
- Instagram App Signature Faking Vulnerabilities (Georg Lukas)

Contact

Please contact Andreas Pfohl (pfohl@rt-solutions.de) or Dr Georg Lukas (lukas@rt-solutions.de) with any further questions regarding the vulnerability.