DroppedIn: Remotely Exploiting the Dropbox SDK for Android

(The CVE-2014-8889 Vulnerability)

TEAM MEMBERS: KEVIN AMORIM, LAMA ALSUWAYAN, HANG XU
Outline

- Goal of the attack
- Android Intents + Dropbox Authentication
- The vulnerability
- DroppedIn Attack
- Mitigation
Data on the Cloud

- World is now storing private personal and business data on the cloud

- Cloud data is not only by the user, but also by apps (photo sharing, storage ... etc.)

- Cloud services often provide a framework (SDK) that apps can utilize
  - Example: The Dropbox SDK for Android
Dropbox API - Stats

Market share overall

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Apps</th>
<th>Installs</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.32%</td>
<td>blue</td>
<td></td>
</tr>
<tr>
<td>1.29%</td>
<td></td>
<td>orange</td>
</tr>
</tbody>
</table>

Market share in top apps

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Apps</th>
<th>Installs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.20%</td>
<td>blue</td>
<td></td>
</tr>
<tr>
<td>3.57%</td>
<td></td>
<td>orange</td>
</tr>
</tbody>
</table>

* Stats according to [AppBrain](https://appbrain.com)
Android & Dropbox

- Android applications execute in a sandbox environment
- Apps can’t access another app’s data directly
- Apps communicate using ‘Intents’
DropBox SDK Authentication (Normal Flow)
DropBox SDK Authentication (Normal Flow)

1. Make nonce & Send Intent

Intent

<table>
<thead>
<tr>
<th>APP ID: App #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extra:</td>
</tr>
<tr>
<td>INTERNAL_WEB_HOST: dropbox.com</td>
</tr>
<tr>
<td>SECRET_nonce: 123456</td>
</tr>
</tbody>
</table>
DropBox SDK Authentication (Normal Flow)

Android

App

SDK

1. Make nonce & Send Intent

Browser

2. Login

Email: example@gmail.com
Password: Required

Log In

New to Dropbox? Create an account

Server

Database

Intent

APP ID: App #

Extra:

INTERNAL_WEB_HOST: dropbox.com
SECRET_nonce: 123456
DropBox SDK Authentication (Normal Flow)

1. Make nonce & Send Intent
2. Login
3. Send info

Intent

<table>
<thead>
<tr>
<th>APP ID: App #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extra:</td>
</tr>
<tr>
<td>INTERNAL_WEB_HOST: dropbox.com</td>
</tr>
<tr>
<td>SECRET_nonce: 123456</td>
</tr>
</tbody>
</table>
DropBox SDK Authentication (Normal Flow)

1. Make nonce & Send Intent
2. Login
3. Send info

Intent

<table>
<thead>
<tr>
<th>APP ID: App #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extra:</td>
</tr>
<tr>
<td>INTERNAL_WEB_HOST: dropbox.com</td>
</tr>
<tr>
<td>SECRET_nonce: 123456</td>
</tr>
</tbody>
</table>
DropBox SDK Authentication (Normal Flow)

1. Make nonce & Send Intent

2. Login

3. Send info

4. Send Access Token

Intent

APP ID: App #

Extra:
INTERNAL_WEB_HOST: dropbox.com
SECRET_nonce: 123456
DropBox SDK Authentication (Normal Flow)

1. Make nonce & Send Intent
2. Login
3. Send info
4. Send Access Token
5. Intent with Access Token and nonce

Intent:
- APP ID: App #
- Extra:
  - INTERNAL_WEB_HOST: dropbox.com
  - SECRET_nonce: 123456
  - ACCESS_TOKEN: 321
DropBox SDK Authentication (Normal Flow)

1. Make nonce & Send Intent

5. Intent with Access Token and nonce

Logged in

Intent

APP ID: App #

Extra:
INTERNAL_WEB_HOST: dropbox.com
SECRET_nonce: 123456
ACCESS_TOKEN: 321
DroppedIn Attack

- Link the app with the attacker’s account instead of the victim’s to either:
  - have the victim upload sensitive information or
  - download malicious, attacker-controlled data that may be used as part of other attacks.

The field “INTERNAL_WEB_HOST” allows this to occur

***Only works when DropBox App is NOT Installed***
DroppedIn Attack

Android

App

SDK

Browser

Bad Page

Server

App ID: #
Atk Token: 666

Server

Intent

APP ID: App #

Extra:
INTERNAL_WEB_HOST:
SECRET_nonce:
ACCESS_TOKEN:
**DroppedIn Attack**

1. Naive Browsing

**Intent**

```
APP ID: App #
Extra:
INTERNAL_WEB_HOST: -
SECRET_nonce: -
ACCESS_TOKEN: -
```
DroppedIn Attack

1. Naive Browsing
2. Exploit

App ID: #
Atk Token: 666

Intent

APP ID: App #
Extra:
INTERNAL_WEB_HOST: <ATTACKER.COM>
SECRET_nonce:
ACCESS_TOKEN:
DroppedIn Attack

1. Naive Browsing
2. Exploit
3. Intent to App

Intent

APP ID: App #
Extra:
INTERNAL_WEB_HOST: attacker.com
SECRET_nonce: 
ACCESS_TOKEN: 

Android

App

SDK

Browser

Bad Page

Server

App ID: #
Atk Token: 666

Database
DroppedIn Attack

Android

App

SDK

Browser

Bad Page

1. Naive Browsing

2. Exploit

3. Intent to App

4. Intent with nonce

Server

App ID: #

Atk Token: 666

Server

Database

Intent

APP ID: App #

Extra:

INTERNAL_WEB_HOST: attacker.com

SECRET_nonce:

-123456

ACCESS_TOKEN:
DroppedIn Attack

1. Naive Browsing
2. Exploit
3. Intent to App
4. Intent with nonce
5. Sends nonce

Server: App ID: # Atk Token: 666

Intent

- APP ID: App #
- Extra:
  - INTERNAL_WEB_HOST: -attacker.com
  - SECRET_nonce: -123456
  - ACCESS_TOKEN: -
DroppedIn Attack

1. Naive Browsing
2. Exploit
3. Intent to App
4. Intent with nonce
5. Sends nonce
6. Sends Atk Token with nonce

APP ID: App #
Extra:
INTERNAL_WEB_HOST: -attacker.com
SECRET_nonce: -123456
ACCESS_TOKEN: -
**DroppedIn Attack**

1. Naive Browsing
2. Exploit
3. Intent to App
4. Intent with nonce
5. Sends nonce
6. Sends Atk Token with nonce

**Intent**

- APP ID: App #
- Extra:
  - INTERNAL_WEB_HOST: attacker.com
- SECRET_nonce: 123456
- ACCESS_TOKEN: 666
Response from Dropbox

- December 1, 2014 - Vulnerabilities disclosed to Dropbox.
- December 2, 2014 - Dropbox confirmed issue, started working on patch.
- December 5, 2014 - Patch available (Dropbox SDK for Android version 1.6.2)
- March 11, 2015 - Public disclosure
Mitigation

- Authentication no longer accepts input parameters from Intent’s extras
  - Don’t allow inputs for INTERNAL_WEB_HOST
- As a developer:
  - Update Dropbox SDK for Android to Version 1.6.2 or higher
- As a user:
  - Install Dropbox onto your android device
  - Make sure you update your apps to their most recent version
References

- http://ibm.co/1Hosb02