MOBSF

ANDROID STATIC ANALYSIS REPORT

ownCloud (4.3.0)

File Name:	owncloud.apk
Package Name:	com.owncloud.android
Scan Date:	Dec. 13, 2024, 12:29 p.m.
App Security Score:	45/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	16	2	2	1

FILE INFORMATION

File Name: owncloud.apk
Size: 13.39MB
MD5: a2c481fad212632c086d050de7f148a1
SHA1: 64cb2011a5022a712908b9b2e0e1dacb75c1a501
SHA256: 615182b69fa8ba9b5111b3cdd5f7ddaf5e6ccd35400a847674c2dd7dc69715df

APP INFORMATION

App Name: ownCloud
Package Name: com.owncloud.android
Main Activity: com.owncloud.android.ui.activity.SplashActivity
Target SDK: 33
Min SDK: 24
Max SDK:
Android Version Name: 4.3.0
Android Version Code: 43000000

APP COMPONENTS

Activities: 21
Services: 8
Receivers: 8
Providers: 5
Exported Activities: 2
Exported Services: 3
Exported Receivers: 1
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=MA, L=Boston, O=ownCloud, OU=com, CN=owncloud.com
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-06-25 17:26:55+00:00
Valid To: 2039-11-11 17:26:55+00:00
Issuer: C=US, ST=MA, L=Boston, O=ownCloud, OU=com, CN=owncloud.com
Serial Number: 0x4fe89f5f
Hash Algorithm: sha1
md5: 7483624935ae9f80f53e5fc89382e6b0
sha1: ff86703ea6e4b8ab61f247218e9d4c95948f6428
sha256: a1b7bfc3cd5dc785bd8680845d5014c6f08944ae49ca031a9e7d5e0a37b182d0
sha512: 33a52bb759318e5880eaab4773a19b18ed8e28ae93c52e3792b6566505f9d48f419a8e5c2d4c715a2a08a02179d0f7a6ba1bdf7644c8d9e2f0c103c318fe84a6
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: fadd622f7b7285320f9fdab800e94d762d2e2b1ad308fd95419d33ac9b60e1a1
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_SYNC_STATS	normal	read sync statistics	Allows an application to read the sync stats; e.g. the history of syncs that have occurred.
android.permission.READ_SYNC_SETTINGS	normal	read sync settings	Allows an application to read the sync settings, such as whether sync is enabled for Contacts.
android.permission.WRITE_SYNC_SETTINGS	normal	write sync settings	Allows an application to modify the sync settings, such as whether sync is enabled for Contacts.
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.owncloud.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.owncloud.android.presentation.authentication.LoginActivity	Schemes: @string/oauth2_redirect_uri_scheme://, @string/deep_link_uri_schemes://, Hosts: @string/oauth2_redirect_uri_path,

NETWORK SECURITY

HIGH: 2 | WARNING: 1 | INFO: 0 | SECURE: 0

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	high	Base config is configured to trust user installed certificates.
3	*	warning	Base config is configured to trust system certificates.

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 7 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Activity (com.owncloud.android.ui.activity.ReceiveExternalFilesActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Service (com.owncloud.android.presentation.authentication.AccountAuthenticatorService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Service (com.owncloud.android.syncadapter.FileSyncService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Content Provider (com.owncloud.android.presentation.documentsprovider.DocumentsStorageProvider) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.MANAGE_DOCUMENTS [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
7	Activity (com.owncloud.android.presentation.authentication.LoginActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
9	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 7 | INFO: 2 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				coil/memory/MemoryCache.java coil/memory/MemoryCacheService.java coil/request/Parameters.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.java com/owncloud/android/data/authentication/AuthenticationConstantsKt.java com/owncloud/android/db/ProviderMeta.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/owncloud/android/domain/authentication/oauth/model/ClientRegistrationInfo.java com/owncloud/android/domain/authentication/usecases/LoginBasicAsyncUseCase.java com/owncloud/android/domain/authentication/usecases/LoginOAuthAsyncUseCase.java com/owncloud/android/domain/sharing/shares/usecases/CreatePublicShareAsyncUseCase.java com/owncloud/android/domain/sharing/shares/usecases/EditPublicShareAsyncUseCase.java com/owncloud/android/domain/webfinger/usecases/GetOwnCloudInstancesFromAuthenticatedWebFingerUseCase.java com/owncloud/android/lib/common/http/HttpConstants.java com/owncloud/android/lib/common/network/NetworkUtils.java com/owncloud/android/lib/resources/oauth/responses/ClientRegistrationResponse.java com/owncloud/android/lib/resources/shares/CreateRemoteShareOperation.java com/owncloud/android/lib/resources/shares/UpdateRemoteShareOperation.java com/owncloud/android/lib/resources/status/responses/FileSharingPublic.java com/owncloud/android/presentation/files/createfolder/CreateFolderDialogFragment.java com/owncloud/android/presentation/files/renamefile/RenameFileDialogFragment.java com/owncloud/android/ui/preview/PreviewFormatTextFragmentStateAdapter.java io/noties/markwon/html/CssProperty.java io/noties/markwon/html/jsoup/nodes/DocumentType.java
				com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFile

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	Loader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/ResourceUriLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/DefaultOnHeaderDecodedListener.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/manager/SingletonConnectivityReceiver.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/caverock/androidsvg/CSSParser.java com/caverock/androidsvg/SVG.java com/caverock/androidsvg/SVGAndroidRenderer.java com/caverock/androidsvg/SVGImageView.java com/caverock/androidsvg/SVGParser.java com/caverock/androidsvg/SimpleAssetResolver.java com/jakewharton/disklrucache/DiskLruCache.java com/owncloud/android/lib/common/utils/OCFileLoggingTree.java io/noties/markwon/LinkResolverDef.java io/noties/markwon/PrecomputedTextSetterCompat.java org/koin/android/logger/AndroidLogger.java timber/log/Timber.java
3	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/owncloud/android/presentation/settings/SettingsFragment.java com/owncloud/android/presentation/sharing/shares/PublicShareDialogFragment.java com/owncloud/android/ui/activity/CopyToClipboardActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/andrognito/patternlockview/utils/PatternLockUtils.java com/owncloud/android/utils/BitmapUtils.java com/owncloud/android/utils/SecurityUtils.java
5	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/andrognito/patternlockview/utils/PatternLockUtils.java
6	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/owncloud/android/presentation/security/biometric/BiometricViewModel.java
7	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/andrognito/patternlockview/utils/RandomUtils.java com/owncloud/android/lib/common/utils/RandomUtils.java com/owncloud/android/utils/NotificationUtils.java
8	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/owncloud/android/data/providers/LegacyStorageProvider.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/owncloud/android/data/migrations/Migration_33Kt.java com/owncloud/android/providers/FileContentProvider.java
10	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	coil/decode/SourceImageSource.java com/owncloud/android/ui/helpers/FilesUploadHelper.java
11	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/owncloud/android/lib/common/network/AdvancedX509TrustManager.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java
00022	Open a file from given absolute path of the file	file	coil/disk/DiskCache.java com/owncloud/android/data/providers/LocalStorageProvider.java com/owncloud/android/datamodel/ThumbnailsCacheManager.java com/owncloud/android/lib/common/network/ChunkFromFileRequestBody.java com/owncloud/android/lib/common/network/FileRequestBody.java com/owncloud/android/lib/common/network/NetworkUtils.java com/owncloud/android/presentation/files/filelist/MainFileListFragment.java com/owncloud/android/ui/activity/ReceiveExternalFilesActivity.java com/owncloud/android/ui/helpers/FilesUploadHelper.java com/owncloud/android/usecases/transfers/uploads/UploadFileInConflictUseCase.java com/owncloud/android/usecases/transfers/uploads/UploadFilesFromSystemUseCase.java com/owncloud/android/workers/DownloadFileWorker.java
00091	Retrieve data from broadcast	collection	com/owncloud/android/presentation/authentication/LoginActivity.java com/owncloud/android/presentation/security/passcode/PassCodeActivity.java com/owncloud/android/presentation/security/pattern/PatternActivity.java
00189	Get the content of a SMS message	sms	com/owncloud/android/lib/common/network/ContentUriRequestBody.java com/owncloud/android/presentation/logging/LogsListActivity.java
00188	Get the address of a SMS message	sms	com/owncloud/android/lib/common/network/ContentUriRequestBody.java com/owncloud/android/presentation/logging/LogsListActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/owncloud/android/lib/common/network/ContentUriRequestBody.java com/owncloud/android/providers/FileContentProvider.java
00191	Get messages in the SMS inbox	sms	com/owncloud/android/lib/common/network/ContentUriRequestBody.java
00200	Query data from the contact list	collection contact	com/owncloud/android/lib/common/network/ContentUriRequestBody.java com/owncloud/android/presentation/logging/LogsListActivity.java
00201	Query data from the call log	collection calllog	com/owncloud/android/lib/common/network/ContentUriRequestBody.java com/owncloud/android/presentation/logging/LogsListActivity.java
00125	Check if the given file path exist	file	com/owncloud/android/presentation/transfers/TransferListFragment.java com/owncloud/android/ui/activity/FileDisplayActivity.java
00013	Read file and put it into a stream	file	coil/fetch/ContentUriFetcher.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/resource/bitmap/ImageReader.java com/jakewharton/disklrucache/DiskLruCache.java com/owncloud/android/lib/common/network/NetworkUtils.java com/owncloud/android/presentation/logging/LogsListActivity.java com/owncloud/android/ui/preview/PreviewTextFragment.java okio/Okio__JvmOkioKt.java
00128	Query user account information	collection account	com/owncloud/android/ui/activity/DrawerActivity.java
00054	Install other APKs from file	reflection	com/owncloud/android/ui/activity/UploadListActivity.java
00036	Get resource file from res/raw directory	reflection	coil/map/ResourceIntMapper.java com/owncloud/android/extensions/ActivityExtKt.java io/noties/markwon/LinkResolverDef.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/owncloud/android/presentation/logging/LogsListActivity.java com/owncloud/android/providers/FileContentProvider.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/owncloud/android/extensions/ActivityExtKt.java com/owncloud/android/presentation/authentication/LoginActivity.java com/owncloud/android/services/OperationsService.java io/noties/markwon/LinkResolverDef.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/owncloud/android/providers/FileContentProvider.java com/owncloud/android/workers/UploadFileFromContentUriWorker.java
00028	Read file from assets directory	file	com/caverock/androidsvg/SimpleAssetResolver.java
00187	Query a URI and check the result	collection sms calllog calendar	com/owncloud/android/providers/FileContentProvider.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/owncloud/android/extensions/ActivityExtKt.java com/owncloud/android/presentation/authentication/LoginActivity.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.WRITE_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	2/44	android.permission.BROADCAST_STICKY, android.permission.FOREGROUND_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
xml.org	ok	**IP:** 104.239.240.11 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
owncloud.com	ok	**IP:** 185.125.174.106 **Country:** Germany **Region:** Bayern **City:** Am See **Latitude:** 47.737881 **Longitude:** 11.737600 **View:** Google Map
calendarserver.org	ok	**IP:** 17.253.23.201 **Country:** United States of America **Region:** Colorado **City:** Denver **Latitude:** 39.739151 **Longitude:** -104.984703 **View:** Google Map
central.owncloud.org	ok	**IP:** 91.107.236.207 **Country:** Iran (Islamic Republic of) **Region:** Tehran **City:** Tehran **Latitude:** 35.694389 **Longitude:** 51.421509 **View:** Google Map
sabredav.org	ok	**IP:** 52.219.208.20 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
owncloud.org	ok	**IP:** 185.125.174.106 **Country:** Germany **Region:** Bayern **City:** Am See **Latitude:** 47.737881 **Longitude:** 11.737600 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
openid.net	ok	**IP:** 140.211.9.53 **Country:** United States of America **Region:** Oregon **City:** Eugene **Latitude:** 44.036083 **Longitude:** -123.052429 **View:** Google Map
play.google.com	ok	**IP:** 142.250.182.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
android.asset	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 20.207.73.82 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
apple.com	ok	**IP:** 17.253.144.10 **Country:** United States of America **Region:** California **City:** Cupertino **Latitude:** 37.316605 **Longitude:** -122.046486 **View:** Google Map
talk.owncloud.com	ok	**IP:** 116.203.190.166 **Country:** Germany **Region:** Bayern **City:** Gunzenhausen **Latitude:** 48.323330 **Longitude:** 11.601220 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
doc.owncloud.com	ok	**IP:** 159.69.243.56 **Country:** Germany **Region:** Sachsen **City:** Falkenstein **Latitude:** 50.477879 **Longitude:** 12.371290 **View:** Google Map
webfinger.owncloud	ok	No Geolocation information available.

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"auth_password" : "Password"
"auth_username" : "Username"
"document_provider_authority" : "org.owncloud.documents"
"file_provider_authority" : "org.owncloud.files"
"oauth2_client_id" : "e4rAsNUSIUs0lF4nbv9FmCeUkTlV9GdgTLDH1b5uie7syb90SzEVrbN7HIpmWJeD"
"oauth2_client_secret" : "dInFYGV33xKzhbRmpqQltYNdfLdJIfJ9L5ISoKhNoT9qZftpdWSP71VrpGR9pmoD"
"oauth2_redirect_uri_path" : "android.owncloud.com"

POSSIBLE SECRETS
"oauth2_redirect_uri_scheme" : "oc"
"oauth2_url_endpoint_access" : "index.php/apps/oauth2/api/v1/token"
"oauth2_url_endpoint_auth" : "index.php/apps/oauth2/authorize"
"search_suggest_authority" : "org.owncloud.search.users_and_groups"
"share_via_link_default_password" : "*****"
"username" : "Username"
"auth_password" : "Contrasenya"
"share_via_link_default_password" : "****"
"auth_password" : "Kodeord"
"auth_username" : "Brugernavn"
"share_via_link_default_password" : "*****"
"username" : "Brugernavn"
"auth_oauth_failure_snackbar_action" : "ورود"
"auth_password" : "گذرواژه"
"share_via_link_default_password" : "*****"

POSSIBLE SECRETS
"auth_password" : "პაროლი"
"auth_password" : "[redacted]"
"auth_username" : "[redacted]"
"username" : "[redacted]"
"auth_oauth_failure_snackbar_action" : "Einloggen"
"auth_password" : "Passwort"
"auth_username" : "Benutzername"
"share_via_link_default_password" : "*****"
"username" : "Benutzername"
"auth_password" : "[redacted]"
"auth_password" : "[redacted]"
"auth_password" : "Лозинка"
"auth_oauth_failure_snackbar_action" : "Ввійти..."
"auth_password" : "Пароль"
"share_via_link_default_password" : "*****"

POSSIBLE SECRETS
"auth_oauth_failure_snackbar_action" : "Συνδεθείτε"
"auth_password" : "Συνθηματικό"
"share_via_link_default_password" : "*****"
"auth_oauth_failure_snackbar_action" : "Rexistrarse"
"auth_password" : "Contrasinal"
"share_via_link_default_password" : "*****"
"auth_oauth_failure_snackbar_action" : "Inloggen"
"auth_password" : "Wachtwoord"
"auth_username" : "Gebruikersnaam"
"share_via_link_default_password" : "*****"
"username" : "Gebruikersnaam"
"auth_oauth_failure_snackbar_action" : "Zaloguj"
"auth_password" : "Hasło"
"share_via_link_default_password" : "*****"
"username" : "Użytkownik"

POSSIBLE SECRETS
"auth_oauth_failure_snackbar_action" : "Prijava"
"auth_password" : "Geslo"
"share_via_link_default_password" : "*****"
"auth_password" : "■■■■■■■■■■■■"
"auth_username" : "■■■■■■■■■■■■■■■■"
"auth_oauth_failure_snackbar_action" : "□□□"
"auth_password" : "□□"
"share_via_link_default_password" : "*****"
"auth_oauth_failure_snackbar_action" : "Înregistraţi-vă"
"auth_password" : "Parolă"
"share_via_link_default_password" : "*****"
"username" : "Utilizator"
"auth_oauth_failure_snackbar_action" : "Hyni"
"auth_password" : "Fjalëkalim"
"share_via_link_default_password" : "*****"

POSSIBLE SECRETS
"share_via_link_default_password" : "*****"
"share_via_link_default_password" : "*****"
"auth_password" : "Lozinka"
"auth_password" : "Лозинка"
"auth_password" : "Parola"
"share_via_link_default_password" : "*****"
"auth_password" : "Lozinka"
"auth_oauth_failure_snackbar_action" : "Registrarse"
"auth_password" : "Contraseña"
"share_via_link_default_password" : "*****"
"auth_password" : "Lykilorð"
"auth_username" : "Notandanafn"
"share_via_link_default_password" : "*****"
"username" : "Notandanafn"
"auth_oauth_failure_snackbar_action" : "Accedi"

POSSIBLE SECRETS
"auth_password" : "Password"
"share_via_link_default_password" : "******"
"auth_password" : "Pasahitza"
"auth_oauth_failure_snackbar_action" : "Войти"
"auth_password" : "Пароль"
"share_via_link_default_password" : "*****"
"auth_password" : "Parole"
"auth_username" : "Lietotājvārds"
"username" : "Lietotājvārds"
"auth_password" : "Lösenord"
"auth_username" : "Användarnamn"
"share_via_link_default_password" : "*****"
"username" : "Användarnamn"
"auth_password" : "Գաղտնաբառ"
"auth_username" : "Օգտանուն"

POSSIBLE SECRETS
"username" : "Օգտանուն"
"auth_password" : "■■■■■□■□"
"auth_username" : "■■■■■□■■■■■□"
"auth_password" : "Şifrə"
"auth_password" : "Password"
"auth_username" : "Username"
"share_via_link_default_password" : "*****"
"username" : "Username"
"auth_password" : "□□"
"auth_username" : "□□□□"
"auth_can_not_auth_against_server" : "□□□□□□□□□□"
"auth_connecting_auth_server" : "□□□□□□□□..."
"auth_expired_basic_auth_toast" : "□□□□□□□□□"
"auth_expired_oauth_token_toast" : "□□□□□□□□□□□□□□□□□"
"auth_fail_get_user_name" : "□□□□□□□□□□□□□□□□□□□ID□□□□□□□□"

POSSIBLE SECRETS
"auth_getting_authorization" : "□□□□..."
"auth_oauth_failure" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"auth_oauth_failure_snackbar_action" : "□□"
"auth_password" : "□□"
"auth_unsupported_auth_method" : "□□□□□□□□□□□□□□□□"
"auth_username" : "□□□"
"oauth_check_onoff" : "□□oAuth2□□"
"share_link_no_support_share_api" : "□□□□□□□□□□□□□□□□□□□□□□□□"
"share_via_link_default_password" : "*****"
"username" : "□□□"
"wait_checking_credentials" : "□□□□□□□□□□□□"
"wait_for_tmp_copy_from_private_storage" : "□□□□□□□□□□□□"
"auth_password" : "Palavra-passe"
"share_via_link_default_password" : "*****"
"auth_can_not_auth_against_server" : "□□□□□□□□□□□□"

POSSIBLE SECRETS
"auth_connecting_auth_server" : "□□□□□□□□□□..."
"auth_expired_basic_auth_toast" : "□□□□□□□□□□"
"auth_getting_authorization" : "□□□□..."
"auth_oauth_failure_snackbar_action" : "□□"
"auth_password" : "□□"
"auth_unsupported_auth_method" : "□□□□□□□□□□□□□□□"
"auth_username" : "□□□□□□"
"oauth_login_connection" : "□□□□□□OAuth2□□□□..."
"share_via_link_default_password" : "*****"
"username" : "□□□□□□"
"wait_checking_credentials" : "□□□□□□□□"
"wait_for_tmp_copy_from_private_storage" : "□□□□□□□□□□□□□□□"
"auth_password" : "Contraseña"
"auth_password" : "Senhal"
"auth_oauth_failure_snackbar_action" : "Masuk"

POSSIBLE SECRETS
"auth_password" : "Sandi"
"share_via_link_default_password" : "*****"
"auth_oauth_failure_snackbar_action" : "התחברות"
"auth_password" : "סמה"
"share_via_link_default_password" : "*****"
"auth_oauth_failure_snackbar_action" : "Anmelden"
"auth_password" : "Passwort"
"auth_username" : "Benutzername"
"share_via_link_default_password" : "*****"
"username" : "Benutzername"
"auth_getting_authorization" : "Autoriseerin..."
"auth_password" : "Parool"
"auth_username" : "Kasutajanimi"
"share_via_link_default_password" : "*****"
"username" : "Kasutajanimi"

POSSIBLE SECRETS
"auth_oauth_failure_snackbar_action" : "Регистрация"
"auth_password" : "Парола"
"share_via_link_default_password" : "*****"
"auth_oauth_failure_snackbar_action" : "Einloggen"
"auth_password" : "Passwort"
"auth_username" : "Benutzername"
"share_via_link_default_password" : "*****"
"username" : "Benutzername"
"auth_can_not_auth_against_server" : "[redacted]"
"auth_connecting_auth_server" : "[redacted]"
"auth_expired_basic_auth_toast" : "[redacted]"
"auth_getting_authorization" : "[redacted]"
"auth_oauth_failure_snackbar_action" : "[redacted]"
"auth_password" : "[redacted]"
"auth_unsupported_auth_method" : "[redacted]"

POSSIBLE SECRETS
"auth_username" : "■■■■■■■■■■"
"share_via_link_default_password" : "*****"
"username" : "■■■■■■■■■■"
"wait_checking_credentials" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"wait_for_tmp_copy_from_private_storage" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"auth_oauth_failure_snackbar_action" : "Kirjaudu"
"auth_password" : "Salasana"
"auth_username" : "Käyttäjätunnus"
"username" : "Käyttäjätunnus"
"auth_password" : "Passord"
"auth_username" : "Brukernavn"
"share_via_link_default_password" : "*****"
"username" : "Brukernavn"
"auth_can_not_auth_against_server" : "□□□□□□□□□□□□□□□□"
"auth_connecting_auth_server" : "□□□□□□□□□□□□..."

POSSIBLE SECRETS
"auth_expired_basic_auth_toast" : "□□□□□□□□□□□□□□□□□□"
"auth_expired_oauth_token_toast" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"auth_fail_get_user_name" : "□□□□□□□□□□□□□ID□□□□□□□□□□□□□□□□□□□□□"
"auth_getting_authorization" : "□□□..."
"auth_oauth_failure" : "□□□"
"auth_oauth_failure_snackbar_action" : "□□□□"
"auth_password" : "□□□□□"
"auth_unsupported_auth_method" : "□□□□□□□□□□□□□□□□□□□□□□□"
"auth_username" : "□□□□□"
"oauth_check_onoff" : "oAuth2□□□□□"
"oauth_login_connection" : "OAuth2□□□□□□□□..."
"share_via_link_default_password" : "*****"
"username" : "□□□□□"
"wait_checking_credentials" : "□□□□□□□□□□□□□□"
"wait_for_tmp_copy_from_private_storage" : "□□□□□□□□□□□□□□□□□□□□□□□"

POSSIBLE SECRETS
"auth_oauth_failure_snackbar_action" : "Entrar"
"auth_password" : "Contraseña"
"share_via_link_default_password" : "*****"
"auth_oauth_failure_snackbar_action" : "Entrar"
"auth_password" : "Senha"
"share_via_link_default_password" : "*****"
"auth_username" : "Identifiant"
"share_via_link_default_password" : "*****"
"username" : "Identifiant"
"auth_oauth_failure_snackbar_action" : "Bejelentkezés"
"auth_password" : "Jelszó"
"auth_username" : "Felhasználónév"
"share_via_link_default_password" : "*****"
"username" : "Felhasználónév"
"auth_password" : "Contraseña"

POSSIBLE SECRETS
"share_via_link_default_password" : "*****"
"auth_oauth_failure_snackbar_action" : "Přihlásit"
"auth_password" : "Heslo"
"share_via_link_default_password" : "*****"
"auth_password" : "Contrasigno"
"auth_password" : "Passwuert"
"auth_username" : "Benotzernumm"
"username" : "Benotzernumm"
"auth_password" : "ئىم"
"auth_password" : "Pasvorto"
"auth_username" : "Uzantonomo"
"username" : "Uzantonomo"
"auth_password" : "Wagwoord"
"auth_username" : "Gebruikersnaam"
"auth_password" : "Cyfrinair"

POSSIBLE SECRETS
"auth_password" : "■■■■■■■"
"auth_username" : "■■■■■■■■■■■"
"auth_password" : "პაროლი"
"auth_password" : "■■■■■■■■■■■"
"auth_password" : "پاسورڈ"
"auth_oauth_failure_snackbar_action" : "Prihlásenie"
"auth_password" : "Heslo"
"share_via_link_default_password" : "*****"
"auth_password" : "Clave"
"auth_username" : "Usuario"
"auth_password" : "Passord"
"auth_username" : "Brukarnamn"
"auth_password" : "Lozinka"
"auth_password" : "Passwort"
"auth_username" : "Benutzername"

POSSIBLE SECRETS
"auth_oauth_failure_snackbar_action" : "Prisijungti"
"auth_password" : "Slaptažodis"
"share_via_link_default_password" : "*****"
"auth_oauth_failure_snackbar_action" : "Войти"
"auth_password" : "Пароль"
"auth_username" : "Пользователь"
"share_via_link_default_password" : "*****"
"username" : "Пользователь"
5181942b9ebc31ce68dacb56c16fd79f
df420cd3391592d9433f0bc74d0a7cce
a0ca6a90-a365-4782-871e-d44447bbc668
8301cb3e334343ef4530fa2f4d7c3bb3
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
ae2044fb577e65ee8bb576ca48a2f06e

PLAYSTORE INFORMATION

Title: ownCloud

Score: 4.16 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Productivity **Play Store URL:** com.owncloud.android

Developer Details: ownCloud GmbH, ownCloud+GmbH, ownCloud GmbH Rathsbergstr. 17 90411 Nürnberg Germany , http://www.owncloud.com, android-app@owncloud.com,

Release Date: Jul 31, 2012 **Privacy Policy:** Privacy link

Description:

Welcome to the ownCloud Android App – Add an ownCloud server, and have your private file sync and share cloud up and running in no time. Do you need private file sync and share software? Then good news, because the ownCloud Android App enables you to connect Android devices to a private ownCloud Server running in your data center. ownCloud is open source file sync and share software for everyone from individuals operating the free ownCloud server, to large enterprises and service providers operating under the ownCloud Enterprise Subscription. ownCloud provides a safe, secure and compliant file sync and share solution – on servers you control. With the ownCloud Android App you can browse all of your ownCloud synced files, create and edit new files, share these files and folders with co-workers, and keep the contents of those folders in sync across all of your devices. Simply copy a file into a directory on your server and ownCloud does the rest. Whether using a mobile device, a desktop, or the web client, ownCloud provides the ability to put the right files in the right hands at the right time on any device in one simple-to-use, secure, private and controlled solution. After all, with ownCloud, it's Your Cloud, Your Data, Your Way. Should you have any problem connecting or synchronizing with your ownCloud server, please contact us on https://github.com/owncloud/android/issues or check https://central.owncloud.org. Visit us at www.ownCloud.com for more information about ownCloud and the ownCloud Subscriptions. For more information on the free and open source ownCloud Server, visit www.ownCloud.org.

SCAN LOGS

Timestamp	Event	Error
2024-12-13 12:29:58	Generating Hashes	OK
2024-12-13 12:29:58	Extracting APK	OK

2024-12-13 12:29:58	Unzipping	OK
2024-12-13 12:29:59	Parsing APK with androguard	OK
2024-12-13 12:30:00	Extracting APK features using aapt/aapt2	OK
2024-12-13 12:30:01	Getting Hardcoded Certificates/Keystores	OK
2024-12-13 12:30:07	Parsing AndroidManifest.xml	OK
2024-12-13 12:30:07	Extracting Manifest Data	OK
2024-12-13 12:30:07	Manifest Analysis Started	OK
2024-12-13 12:30:07	Reading Network Security config from network_security_config.xml	OK
2024-12-13 12:30:07	Parsing Network Security config	OK
2024-12-13 12:30:07	Performing Static Analysis on: ownCloud (com.owncloud.android)	OK

2024-12-13 12:30:07	Fetching Details from Play Store: com.owncloud.android	OK
2024-12-13 12:30:07	Checking for Malware Permissions	OK
2024-12-13 12:30:07	Fetching icon path	OK
2024-12-13 12:30:07	Library Binary Analysis Started	OK
2024-12-13 12:30:07	Reading Code Signing Certificate	OK
2024-12-13 12:30:08	Running APKiD 2.1.5	OK
2024-12-13 12:30:15	Detecting Trackers	OK
2024-12-13 12:30:21	Decompiling APK to Java with JADX	OK
2024-12-13 12:31:24	Converting DEX to Smali	OK
2024-12-13 12:31:24	Code Analysis Started on - java_source	OK
2024-12-13 12:31:30	Android SBOM Analysis Completed	OK

2024-12-13 12:31:48	Android SAST Completed	OK
2024-12-13 12:31:48	Android API Analysis Started	OK
2024-12-13 12:31:52	Android API Analysis Completed	OK
2024-12-13 12:31:53	Android Permission Mapping Started	OK
2024-12-13 12:31:59	Android Permission Mapping Completed	OK
2024-12-13 12:31:59	Android Behaviour Analysis Started	OK
2024-12-13 12:32:05	Android Behaviour Analysis Completed	OK
2024-12-13 12:32:05	Extracting Emails and URLs from Source Code	OK
2024-12-13 12:32:09	Email and URL Extraction Completed	OK
2024-12-13 12:32:09	Extracting String data from APK	OK
2024-12-13 12:32:10	Extracting String data from Code	OK

2024-12-13 12:32:10	Extracting String values and entropies from Code	OK
2024-12-13 12:32:15	Performing Malware check on extracted domains	OK
2024-12-13 12:32:20	Saving to Database	OK

Report Generated by - MobSF v4.2.9

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.