ANDROID STATIC ANALYSIS REPORT

Nextcloud (3.19.0)

File Name:	Nextcloud.apk
Package Name:	com.nextcloud.client
Scan Date:	March 2, 2022, 10:41 a.m.
App Security Score:	29/100 (CRITICAL RISK)
Grade:	
Trackers Detection:	1/421

FINDINGS SEVERITY

HIGH	WARNING	INFO	SECURE
16	19	2	1

FILE INFORMATION

File Name: Nextcloud.apk
Size: 27.82MB
MD5: bc6b5753d6aaede9e7295f944882d78e
SHA1: 0b60438054aada3b39c6abcdd236e27ae9361e28
SHA256: 6c1203763f0dd627037476e681dc86ce4a368ecf87c7eae5953d3d7bb5d1c665

APP INFORMATION

App Name: Nextcloud
Package Name: com.nextcloud.client
Main Activity: com.owncloud.android.ui.activity.FileDisplayActivity
Target SDK: 30
Min SDK: 23
Max SDK:
Android Version Name: 3.19.0
Android Version Code: 30190090

APP COMPONENTS

Activities: 38
Services: 17
Receivers: 13
Providers: 7
Exported Activities: 6
Exported Services: 4
Exported Receivers: 3
Exported Providers: 3

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: O=Nextcloud
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-06-12 09:10:47+00:00
Valid To: 2041-06-06 09:10:47+00:00
Issuer: O=Nextcloud
Serial Number: 0x7123f384
Hash Algorithm: sha256
md5: 3d2b0d9a8a026b5848429b882b2f950a
sha1: 74aa1702e714941be481e1f7ce4a8f779c19dcea
sha256: fb009522f65e25802261b67b10a45fd70e610031976f40b28a649e152ded0373
sha512: 8f0087ffe31c94b67ef18726b9268b4481942a93ced92f9e0a810a545dff40d358f41934c06cc2ba86106367174e41971168493d4c781f32e2e4c0f395452847
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 96e2ad04bd5dc10182fbc0aa9ff1a90778e575ef9ec08636230f9742ab250da3

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.MANAGE_EXTERNAL_STORAGE	dangerous	Allows an application a broad access to external storage in scoped storage	Allows an application a broad access to external storage in scoped storage. Intended to be used by few apps that need to manage files on behalf of the users.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal		Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)
classes2.dex	FINDINGS: Anti-VM Code — DETAILS: Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)
classes3.dex	FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)
classes4.dex	FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.owncloud.android.authentication.ModifiedAuthenticatorActivity	Schemes: @string/login_data_own_scheme://, Hosts: login,
com.owncloud.android.ui.activity.FileDisplayActivity	Schemes: http://, https://, Hosts: *, Path Patterns: /f/..*, /..*/f/..*, /..*/..*/f/..*, /..*/..*/..*/f/..*,
com.owncloud.android.authentication.DeepLinkLoginActivity	Schemes: @string/login_data_own_scheme://, Hosts: login,

NETWORK SECURITY

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

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
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	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
4	Activity (com.owncloud.android.authentication.ModifiedAuthenticatorActivity) is not Protected. [android:exported=true]	high	An Activity 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.services.firebase.NCFirebaseMessagingService) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Service is explicitly exported.
6	Activity (com.owncloud.android.ui.activity.ReceiveExternalFilesActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Service (com.owncloud.android.syncadapter.FileSyncService) is not Protected. [android:exported=true]	high	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
8	Content Provider (com.owncloud.android.providers.FileContentProvider) is not Protected. [android:exported=true]	high	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.
9	Content Provider (com.owncloud.android.providers.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.
10	Content Provider (com.owncloud.android.providers.DiskLruImageCacheFileProvider) 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.
11	Activity (com.owncloud.android.authentication.AuthenticatorActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Activity (com.owncloud.android.authentication.DeepLinkLoginActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Activity (com.owncloud.android.ui.trashbin.TrashbinActivity) is not Protected. [android:exported=true]	high	An Activity 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
14	Broadcast Receiver (com.owncloud.android.files.BootupBroadcastReceiver) is not Protected. [android:exported=true]	high	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.
15	Service (com.owncloud.android.services.AccountManagerService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
16	Activity (com.owncloud.android.ui.activity.SsoGrantPermissionActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
17	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.
18	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.

NO	ISSUE	SEVERITY	DESCRIPTION
19	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	de/cotech/hw/fido/FidoFacetIdUtil.java com/owncloud/android/utils/EncryptionUtils.java
				com/blikoon/qrcodescanner/camera/PreviewCallback.java com/owncloud/android/lib/resources/comments/CommentFileRemoteOperation.java com/blikoon/qrcodescanner/QrCodeActivity.java freemarker/ext/dom/Transform.java dagger/android/AndroidInjection.java com/owncloud/android/lib/common/OwnCloudClientManager.java com/bumptech/glide/Glide.java com/owncloud/android/ui/activity/FolderPickerActivity.java org/slf4j/helpers/Util.java com/bumptech/glide/load/resource/bitmap/Dow

NO	ISSUE	SEVERITY	STANDARDS	FILES
				nsampler.java org/conscrypt/ct/CTVerifier.java com/owncloud/android/ui/activity/SyncedFoldersActivity.java com/owncloud/android/utils/FileStorageUtils.java com/owncloud/android/lib/resources/trashbin/RestoreTrashbinFileRemoteOperation.java com/caverock/androidsvg/SVGParser.java com/bumptech/glide/load/resource/bitmap/ImageHeaderParser.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/util/ContentLengthInputStream.java com/owncloud/android/lib/common/utils/Log_OC.java com/bumptech/glide/load/engine/EngineRunnable.java com/owncloud/android/utils/GooglePlayUtils.java com/nextcloud/android/sso/InputStreamBinder$$ExternalSyntheticLambda1.java org/conscrypt/Platform.java com/caverock/androidsvg/SVGAndroidRenderer.java com/owncloud/android/ui/adapter/X509CertificateViewAdapter.java com/owncloud/android/lib/resources/files/CopyFileRemoteOperation.java com/bumptech/glide/load/model/StreamEncoder.java io/noties/markwon/LinkResolverDef.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/request/GenericRequest.java com/owncloud/android/utils/PushUtils.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java

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	freemarker/template/utility/ToCanonical.java com/owncloud/android/utils/DisplayUtils.java de/cotech/hw/util/HwTimber.java com/bumptech/glide/load/resource/gif/GifResourceDecoder.java com/owncloud/android/providers/DocumentsStorageProvider.java com/bumptech/glide/load/resource/gif/GifResourceEncoder.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/blikoon/qrcodescanner/camera/CameraConfigurationManager.java com/bumptech/glide/load/engine/CacheLoader.java com/blikoon/qrcodescanner/decode/CaptureActivityHandler.java com/nextcloud/android/sso/InputStreamBinder$$ExternalSyntheticLambda0.java com/owncloud/android/ui/activity/SsoGrantPermissionActivity.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/blikoon/qrcodescanner/camera/AutoFocusCallback.java com/owncloud/android/datamodel/MediaProvider.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/owncloud/android/lib/resources/trashbin/EmptyTrashbinRemoteOperation.java com/bumptech/glide/load/data/MediaStoreThumbFetcher.java com/nextcloud/common/OkHttpMethodBase.java com/caverock/androidsvg/SimpleAssetResolver.java com/bumptech/glide/util/ByteArrayPool.java com/owncloud/android/lib/resources/files/RestoreFileVersionRemoteOperation.java com/owncloud/android/lib/resources/files/MoveFileRemoteOperation.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/caverock/androidsvg/SVGImageView.java com/owncloud/android/ui/helpers/FileOperationsHelper.java com/afollestad/sectionedrecyclerview/SectionedRecyclerViewAdapter.java com/bumptech/glide/load/engine/executor/FifoPriorityThreadPoolExecutor.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/load/resource/bitmap/RecyclableBufferedInputStream.java com/blikoon/qrcodescanner/decode/DecodeManager.java com/bumptech/glide/gifdecoder/GifDecoder.java freemarker/core/CommandLine.java com/bumptech/glide/load/model/ImageVideoModelLoader.java com/nextcloud/client/jobs/NotificationWork.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/caverock/androidsvg/SVG.java com/nextcloud/client/logger/LoggerImpl.java com/bumptech/glide/load/engine/Engine.java com/caverock/androidsvg/CSSParser.java io/noties/markwon/PrecomputedTextSetterCompat.java com/owncloud/android/operations/RefreshFolderOperation.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/manager/RequestManagerFragment.java com/owncloud/android/operations/SynchronizeFolderOperation.java com/bumptech/glide/load/resource/bitmap/ImageVideoBitmapDecoder.java com/owncloud/android/operations/UploadFileOperation.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				edu/emory/mathcs/backport/java/util/concurrent/helpers/Utils.java com/bumptech/glide/gifencoder/AnimatedGifEncoder.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/data/AssetPathFetcher.java
3	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	de/cotech/hw/fido2/internal/operations/ctap1/AutoValue_U2fRegisterResponse.java org/jsoup/nodes/DocumentType.java org/conscrypt/OpenSSLECKeyFactory.java freemarker/template/utility/StandardCompress.java com/nextcloud/android/lib/resources/users/GenerateAppPasswordRemoteOperation.java de/cotech/hw/fido2/domain/create/AutoValue_AttestedCredentialData.java com/owncloud/android/lib/resources/users/SendCSROperation.java com/owncloud/android/lib/resources/notifications/UnregisterAccountDeviceForProxyOperation.java com/owncloud/android/db/ProviderMeta.java com/owncloud/android/lib/resources/users/StorePrivateKeyOperation.java com/owncloud/android/lib/resources/notifications/RegisterAccountDeviceForProxyOperation.java freemarker/log/_Log4jOverSLF4JTester.java de/cotech/hw/fido2/domain/create/AutoValue_AuthenticatorSelectionCriteria.java io/noties/markwon/html/CssProperty.java com/owncloud/android/lib/resources/notifications/RegisterAccountDeviceForNotificationsOperation.java com/owncloud/android/lib/resources/shares/CreateShareRemoteOperation.java org/jsoup/parser/TokeniserState.java freemarker/core/BuiltinVariable.java org/jsoup/helper/W3CDom.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/conscrypt/OpenSSLRSAKeyFactory.java io/noties/markwon/html/jsoup/parser/TokeniserState.java
				com/owncloud/android/lib/resources/shares/ShareXMLParser.java com/owncloud/android/lib/resources/status/GetCapabilitiesRemoteOperation.java io/noties/markwon/html/jsoup/nodes/DocumentType.java com/nextcloud/client/jobs/TestJob.java
4	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/MainApp.java com/owncloud/android/ui/activity/FileDisplayActivity.java com/owncloud/android/utils/FileStorageUtils.java com/owncloud/android/ui/dialog/LocalStoragePathPickerDialogFragment.java com/owncloud/android/ui/activity/UploadFilesActivity.java com/owncloud/android/datamodel/MediaProvider.java com/owncloud/android/ui/helpers/FileOperationsHelper.java com/owncloud/android/datastorage/DataStorageProvider.java com/owncloud/android/ui/fragment/LocalFileListFragment.java
5	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	org/conscrypt/ChainStrengthAnalyzer.java org/conscrypt/OpenSSLECGroupContext.java org/conscrypt/OidData.java org/conscrypt/OpenSSLProvider.java org/conscrypt/CertificatePriorityComparator.java org/conscrypt/OpenSSLCipherRSA.java org/conscrypt/TrustManagerImpl.java org/conscrypt/OAEPParameters.java org/conscrypt/ct/CTConstants.java org/conscrypt/EvpMdRef.java org/conscrypt/OpenSSLSignature.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	org/conscrypt/DefaultSSLContextImpl.java org/conscrypt/SSLParametersImpl.java com/owncloud/android/lib/common/network/AdvancedX509TrustManager.java org/conscrypt/Conscrypt.java
7	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/owncloud/android/lib/resources/files/FileUtils.java com/owncloud/android/utils/BitmapUtils.java com/owncloud/android/utils/EncryptionUtils.java
8	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/utils/ClipboardUtil.java
9	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	de/cotech/hw/internal/transport/usb/ctaphid/CtapHidInitStructFactory.java freemarker/debug/impl/DebuggerServer.java edu/emory/mathcs/backport/java/util/Collections.java org/jsoup/helper/DataUtil.java edu/emory/mathcs/backport/java/util/concurrent/ConcurrentSkipListMap.java com/nextcloud/client/jobs/MediaFoldersDetectionWork.java
10	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/owncloud/android/ui/activity/ExternalSiteWebView.java
11	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	org/lukhnos/nnio/file/Files.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/owncloud/android/authentication/AuthenticatorActivity.java
13	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/providers/FileContentProvider.java
14	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	org/conscrypt/Conscrypt.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/arm64-v8a/libconscrypt_jni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__memmove_chk', '__strchr_chk', '__memset_chk', '__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/arm64-v8a/libpl_droidsonroids_gif.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strncat_chk', '__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/armeabi-v7a/libconscrypt_jni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/armeabi-v7a/libpl_droidsonroids_gif.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strncat_chk', '__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/x86/libconscrypt_jni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	lib/x86/libpl_droidsonroids_gif.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strncat_chk', '__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/x86_64/libconscrypt_jni.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk', '__strchr_chk', '__memcpy_chk', '__memset_chk', '__read_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	lib/x86_64/libpl_droidsonroids_gif.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strncat_chk', '__memcpy_chk']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application implement DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['NFC', 'network connectivity', 'camera'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to ['address book', 'calendar'].
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.
12	FCS_CKM.1.1(3),FCS_CKM.1.2(3)	Selection-Based Security Functional Requirements	Password Conditioning	A password/passphrase shall perform [Password-based Key Derivation Functions] in accordance with a specified cryptographic algorithm..
13	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption not in accordance with FCS_COP.1.1(1), AES-ECB mode is being used.
14	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
15	FCS_COP.1.1(3)	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
16	FCS_COP.1.1(4)	Selection-Based Security Functional Requirements	Cryptographic Operation - Keyed-Hash Message Authentication	The application perform keyed-hash message authentication with cryptographic algorithm ['HMAC-SHA-256'] .

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
17	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
18	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
19	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
20	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The application validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates', 'The application validate the revocation status of the certificate using the Online Certificate Status Protocol (OCSP) as specified in RFC 2560 or a Certificate Revocation List (CRL) as specified in RFC 5759 or an OCSP TLS Status Request Extension (i.e., OCSP stapling) as specified in RFC 6066', 'The certificate path must terminate with a trusted CA certificate', 'RFC 5280 certificate validation and certificate path validation'].
21	FIA_X509_EXT.1.2	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.
22	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
23	FIA_X509_EXT.2.2	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	When the application cannot establish a connection to determine the validity of a certificate, the application allow the administrator to choose whether to accept the certificate in these cases or accept the certificate ,or not accept the certificate.
24	FCS_CKM.1.1(2)	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
download.nextcloud.com	ok	**IP:** 95.217.64.181 **Country:** Finland **Region:** Uusimaa **City:** Helsinki **Latitude:** 60.169521 **Longitude:** 24.935450 **View:** Google Map
www.gnu.org	ok	**IP:** 209.51.188.116 **Country:** United States of America **Region:** Massachusetts **City:** Boston **Latitude:** 42.358429 **Longitude:** -71.059769 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
f-droid.org	ok	**IP:** 148.251.140.42 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
www.w3.org	ok	**IP:** 128.30.52.100 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.365078 **Longitude:** -71.104523 **View:** Google Map
xml.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.transifex.com	ok	**IP:** 52.50.147.82 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
hwsecurity.dev	ok	**IP:** 104.198.14.52 **Country:** United States of America **Region:** Oregon **City:** The Dalles **Latitude:** 45.594559 **Longitude:** -121.178680 **View:** Google Map
apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
push-notifications.nextcloud.com	ok	**IP:** 176.9.217.51 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
www.slf4j.org	ok	**IP:** 83.173.251.158 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.nextcloud.com	ok	**IP:** 95.217.53.153 **Country:** Finland **Region:** Uusimaa **City:** Helsinki **Latitude:** 60.169521 **Longitude:** 24.935450 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.
play.google.com	ok	**IP:** 142.250.199.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.apple.com	ok	**IP:** 124.41.245.22 **Country:** Nepal **Region:** Bagmati **City:** Kathmandu **Latitude:** 27.701691 **Longitude:** 85.320602 **View:** Google Map
goo.gl	ok	**IP:** 142.250.183.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
schemas.android.com	ok	No Geolocation information available.
github.com	ok	**IP:** 20.205.243.166 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
android.asset	ok	No Geolocation information available.
freemarker.org	ok	**IP:** 192.64.119.217 **Country:** United States of America **Region:** Georgia **City:** Atlanta **Latitude:** 33.727291 **Longitude:** -84.425377 **View:** Google Map
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
xmlpull.org	ok	**IP:** 74.50.61.58 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.814899 **Longitude:** -96.879204 **View:** Google Map
help.nextcloud.com	ok	**IP:** 95.217.53.146 **Country:** Finland **Region:** Uusimaa **City:** Helsinki **Latitude:** 60.169521 **Longitude:** 24.935450 **View:** Google Map
nextcloud-a7dea.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
nextcloud.com	ok	**IP:** 95.217.53.153 **Country:** Finland **Region:** Uusimaa **City:** Helsinki **Latitude:** 60.169521 **Longitude:** 24.935450 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
freemarker.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://nextcloud-a7dea.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
appro@openssl.org	lib/arm64-v8a/libconscrypt_jni.so

TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"document_provider_authority" : "org.nextcloud.documents"
"end_to_end_encryption_password" : "Password..."
"etm_background_job_user" : "User"
"etm_transfer_user" : ""
"file_provider_authority" : "org.nextcloud.files"
"firebase_database_url" : "https://nextcloud-a7dea.firebaseio.com"
"google_api_key" : "AIzaSyAWIyOcLafaFp8PFL61h64cy1NNZW2cU_s"
"google_crash_reporting_api_key" : "AIzaSyAWIyOcLafaFp8PFL61h64cy1NNZW2cU_s"
"image_cache_provider_authority" : "org.nextcloud.imageCache.provider"
"share_via_link_unset_password" : "Unset"
"username" : "Username"
"users_and_groups_search_authority" : "com.nextcloud.android.providers.UsersAndGroupsSearchProvider"

POSSIBLE SECRETS
"end_to_end_encryption_password" : "Contrasenya..."
"etm_background_job_user" : "Usuari"
"end_to_end_encryption_password" : "Adgangskode..."
"etm_background_job_user" : "Bruger"
"username" : "Brugernavn"
"etm_background_job_user" : "کاربر"
"end_to_end_encryption_password" : "Crae..."
"etm_background_job_user" : "Utente"
"end_to_end_encryption_password" : "Facal-faire..."
"etm_background_job_user" : "Cleachdaiche"
"share_via_link_unset_password" : "Neo-shuidhich"
"username" : "Ainm-cleachdaiche"
"end_to_end_encryption_password" : "Passwort..."
"etm_background_job_user" : "Benutzer"
"prefs_lock_using_device_credentials" : "Geräte-Anmeldedaten"
"share_via_link_unset_password" : "Entfernen"

POSSIBLE SECRETS
"username" : "Benutzername"
"end_to_end_encryption_password" : "Лозинка..."
"etm_background_job_user" : "Корисник"
"share_via_link_unset_password" : "Непоставено"
"end_to_end_encryption_password" : "Пароль..."
"etm_background_job_user" : "Користувач"
"share_via_link_unset_password" : "Зняти"
"end_to_end_encryption_password" : "Συνθηματικό..."
"etm_background_job_user" : "Χρήστης"
"share_via_link_unset_password" : "Απενεργοποίηση"
"end_to_end_encryption_password" : "Contrasinal..."
"etm_background_job_user" : "Usuario"
"end_to_end_encryption_password" : "Wachtwoord..."
"etm_background_job_user" : "Gebruiker"
"prefs_lock_using_device_credentials" : "Toestelgegevens"
"share_via_link_unset_password" : "uitgeschakeld"

POSSIBLE SECRETS
"username" : "Gebruikersnaam"
"end_to_end_encryption_password" : "Hasło..."
"etm_background_job_user" : "Użytkownik"
"share_via_link_unset_password" : "Nieustalone"
"etm_background_job_user" : "Uporabnik"
"etm_background_job_user" : "Pengguna"
"end_to_end_encryption_password" : "Pasvorto..."
"share_via_link_unset_password" : "Malprotekti"
"username" : "Uzantonomo"
"end_to_end_encryption_password" : " ..."
"etm_background_job_user" : " "
"active_user" : "[redacted]"
"credentials_disabled" : "[redacted]"
"default_credentials_wrong" : "[redacted]"
"end_to_end_encryption_enter_password" : "[redacted]"
"end_to_end_encryption_password" : "[redacted]"

POSSIBLE SECRETS

"etm_background_job_user" : "[redacted]"

"prefs_lock_device_credentials_enabled" : "[redacted]"

"prefs_lock_device_credentials_not_setup" : "[redacted]"

"prefs_lock_using_device_credentials" : "[redacted]"

"share_via_link_unset_password" : "[redacted]"

"username" : "[redacted]"

"wait_checking_credentials" : "[redacted]"

"wait_for_tmp_copy_from_private_storage" : "[redacted]"

"end_to_end_encryption_password" : "Parolă..."

"etm_background_job_user" : "Utilizator"

"share_via_link_unset_password" : "Desetează"

"username" : "Utilizator"

"end_to_end_encryption_password" : "Fjalëkalimi..."

"etm_background_job_user" : "Përdorues"

"etm_background_job_user" : "المستخدم"

"end_to_end_encryption_password" : "Ger-tremen"

POSSIBLE SECRETS
"etm_background_job_user" : "Implijer"
"etm_background_job_user" : "Utilisateur"
"share_via_link_unset_password" : "Désactiver"
"end_to_end_encryption_password" : "Zaporka..."
"etm_background_job_user" : ""
"share_via_link_unset_password" : "Ukloni"
"end_to_end_encryption_password" : "Лозинка..."
"etm_background_job_user" : "Корисник"
"share_via_link_unset_password" : "Уклони"
"etm_background_job_user" : "Kullanıcı"
"share_via_link_unset_password" : "Kaldır"
"end_to_end_encryption_password" : "Contraseña..."
"etm_background_job_user" : "Usuario"
"share_via_link_unset_password" : "Desmarcar"
"end_to_end_encryption_password" : "Lykilorð"
"etm_background_job_user" : "Notandi"

POSSIBLE SECRETS
"share_via_link_unset_password" : "Endurstilla"
"username" : "Notandanafn"
"end_to_end_encryption_password" : "Password..."
"etm_background_job_user" : "Utente"
"share_via_link_unset_password" : "Rimuovi"
"end_to_end_encryption_password" : "Pasahitza..."
"etm_background_job_user" : "Erabiltzailea"
"username" : "Erabiltzaile-izena"
"end_to_end_encryption_password" : "Пароль..."
"etm_background_job_user" : "Пользователь"
"share_via_link_unset_password" : "Сброс"
"end_to_end_encryption_password" : "Parole..."
"share_via_link_unset_password" : "Neuzstādīts"
"username" : "Lietotājvārds"
"end_to_end_encryption_password" : "Lösenord..."
"etm_background_job_user" : "Användare"

POSSIBLE SECRETS
"share_via_link_unset_password" : "Inaktivera"
"username" : "Användarnamn"
"end_to_end_encryption_password" : "ססמה..."
"etm_background_job_user" : "משתמש"
"end_to_end_encryption_password" : "Password..."
"etm_background_job_user" : "User"
"share_via_link_unset_password" : "Unset"
"username" : "Username"
"username" : "Usuario"
"end_to_end_encryption_password" : "Парола..."
"etm_background_job_user" : "Потребител"
"share_via_link_unset_password" : "Анулиране"
"username" : "Потребител"
"end_to_end_encryption_password" : "Salasana..."
"etm_background_job_user" : "Käyttäjä"
"share_via_link_unset_password" : "Poista"

POSSIBLE SECRETS
"username" : "Käyttäjätunnus"
"active_user" : " "
"auth_fail_get_user_name" : " "
"credentials_disabled" : " "
"default_credentials_wrong" : " "
"end_to_end_encryption_enter_password" : " "
"end_to_end_encryption_password" : " ..."
"end_to_end_encryption_wrong_password" : " "
"etm_background_job_user" : " "
"prefs_e2e_no_device_credentials" : " "
"prefs_lock_device_credentials_enabled" : " "
"prefs_lock_device_credentials_not_setup" : " "
"prefs_lock_using_device_credentials" : " "
"share_via_link_unset_password" : " "
"username" : " "
"wait_checking_credentials" : " "

POSSIBLE SECRETS
"wait_for_tmp_copy_from_private_storage" : " "
"end_to_end_encryption_password" : "Heslo..."
"etm_background_job_user" : "Používateľ"
"share_via_link_unset_password" : "Zrušiť"
"active_user" : " "
"auth_fail_get_user_name" : " ID "
"credentials_disabled" : " "
"default_credentials_wrong" : " "
"end_to_end_encryption_enter_password" : " "
"end_to_end_encryption_password" : " ..."
"end_to_end_encryption_wrong_password" : " "
"etm_background_job_user" : " "
"prefs_e2e_no_device_credentials" : " "
"prefs_lock_device_credentials_enabled" : " "
"prefs_lock_device_credentials_not_setup" : " "
"prefs_lock_using_device_credentials" : " "

POSSIBLE SECRETS
"share_via_link_unset_password" : " "
"username" : " "
"wait_checking_credentials" : " "
"wait_for_tmp_copy_from_private_storage" : " "
"end_to_end_encryption_password" : "Passord..."
"etm_background_job_user" : "Bruker"
"username" : "Brukernavn"
"active_user" : " "
"auth_fail_get_user_name" : " ID "
"credentials_disabled" : " "
"default_credentials_wrong" : " "
"end_to_end_encryption_enter_password" : " "
"end_to_end_encryption_password" : " ..."
"end_to_end_encryption_wrong_password" : " ?"
"etm_background_job_user" : " "
"prefs_e2e_no_device_credentials" : " "

POSSIBLE SECRETS
"prefs_lock_device_credentials_enabled" : " "
"prefs_lock_device_credentials_not_setup" : " "
"prefs_lock_using_device_credentials" : " "
"share_via_link_unset_password" : " "
"username" : " "
"wait_checking_credentials" : " "
"wait_for_tmp_copy_from_private_storage" : " "
"end_to_end_encryption_password" : "Lozinka..."
"share_via_link_unset_password" : "Ukloni"
"end_to_end_encryption_password" : "Contraseña..."
"etm_background_job_user" : "Usuario"
"share_via_link_unset_password" : "Desconectado"
"end_to_end_encryption_password" : "Senha..."
"etm_background_job_user" : "Usuário"
"end_to_end_encryption_password" : "Slaptažodis..."
"etm_background_job_user" : "Naudotojas"

POSSIBLE SECRETS
"share_via_link_unset_password" : "Nenustatyta"
"end_to_end_encryption_password" : "Palavra-passe..."
"etm_background_job_user" : "Utilizador"
"share_via_link_unset_password" : "Retirar"
"end_to_end_encryption_password" : "Jelszó..."
"etm_background_job_user" : "Felhasználó"
"prefs_lock_using_device_credentials" : "Eszközhitelesítő-adatok"
"share_via_link_unset_password" : "Kikapcsolás"
"username" : "Felhasználónév"
"active_user" : " "
"auth_fail_get_user_name" : " "
"credentials_disabled" : " "
"default_credentials_wrong" : " "
"end_to_end_encryption_enter_password" : " "
"end_to_end_encryption_password" : " ....."
"end_to_end_encryption_wrong_password" : " "

POSSIBLE SECRETS
"etm_background_job_user" : " "
"prefs_e2e_no_device_credentials" : " "
"prefs_lock_device_credentials_enabled" : " "
"prefs_lock_device_credentials_not_setup" : " "
"prefs_lock_using_device_credentials" : " "
"share_via_link_unset_password" : " "
"username" : " "
"wait_checking_credentials" : " "
"wait_for_tmp_copy_from_private_storage" : " "
"end_to_end_encryption_password" : "Heslo..."
"etm_background_job_user" : "Uživatel"
"etm_background_job_user" : "Ulanyjy"
"share_via_link_unset_password" : "Gurnalmady"
"end_to_end_encryption_password" : "Contraseña..."
"username" : "Usuario"
"end_to_end_encryption_password" : "Contraseña..."

POSSIBLE SECRETS
"username" : "Usuario"
"end_to_end_encryption_password" : "Contraseña..."
"username" : "Usuario"
"end_to_end_encryption_password" : "Contraseña..."
"username" : "Usuario"
"end_to_end_encryption_password" : "Contraseña..."
"username" : "Usuario"
"end_to_end_encryption_password" : "Contraseña..."
"username" : "Usuario"
"end_to_end_encryption_password" : "Contraseña..."
"username" : "Usuario"
"end_to_end_encryption_password" : "Contraseña..."
"etm_background_job_user" : "Usuario"
"share_via_link_unset_password" : "Desestablecer"
"username" : "Usuario"
"username" : "Usuario"

PLAYSTORE INFORMATION

Title: Nextcloud

Score: 3.68 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** 6.0 and up **Category:** Productivity **Play Store URL:** com.nextcloud.client

Developer Details: Nextcloud, Nextcloud, Nextcloud GmbH Hauptmannsreute 44A 70192 Stuttgart Germany, https://nextcloud.com, android@nextcloud.com,

Release Date: Jun 12, 2016 **Privacy Policy:** Privacy link

Description:

The Open Source Nextcloud Android app allows you to access all your files on your Nextcloud. Features: * Easy, modern interface * Upload your files to your Nextcloud server * Share your files with others * Keep your favorite files and folders synced * Instant Upload for photos and videos taken by your device * Multi-account support Please report all issues at https://github.com/nextcloud/android/issues and discuss this app at https://help.nextcloud.com ;-) New to Nextcloud? Nextcloud is a private file sync & share and communication server. It is fully open source and you can host it yourself or pay a company to do it for you. That way, you are in control of your photos, your calendar and contact data, your documents and everything else. Check out Nextcloud at https://nextcloud.com

---

Report Generated by - MobSF v3.5.1 Beta

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.