



# ANDROID STATIC ANALYSIS REPORT



 CTT (1.0.960)

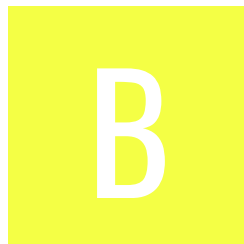
File Name: ctt\_pulled.apk

Package Name: pt.ctt.outsystems.CTT

Scan Date: Feb. 25, 2023, 5:05 p.m.






App Security Score: 50/100 (MEDIUM RISK)

Grade:



Trackers Detection: 2/428

## FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
0	13	1	0	1

## FILE INFORMATION

**File Name:** ctt\_pulled.apk

**Size:** 26.68MB

**MD5:** b05a371b67bddbc970fdabb2689da2e2

**SHA1:** 4a168d9e7e5164d7296ae69a6d954f8ecef04d7a

**SHA256:** 12ffe788570834ac5d458f64849e9e8443a92ae0cfe686a99e780ecd66c2f0e5

## APP INFORMATION

**App Name:** CTT

**Package Name:** pt.ctt.outsystems.CTT

**Main Activity:** pt.ctt.outsystems.CTT.MainActivity

**Target SDK:** 33

**Min SDK:** 26

**Max SDK:**

**Android Version Name:** 1.0.960

Android Version Code: 95

## APP COMPONENTS

Activities: 7

Services: 12

Receivers: 6

Providers: 3

Exported Activities: 1

Exported Services: 3

Exported Receivers: 6

Exported Providers: 0

## CERTIFICATE INFORMATION

APK is signed

v1 signature: False

v2 signature: True

v3 signature: True

Found 1 unique certificates

Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Signature Algorithm: rsassa\_pkcs1v15

Valid From: 2022-10-19 18:13:33+00:00

Valid To: 2052-10-19 18:13:33+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0x606570053a98bf05ff470d150541011b32e96ebc

Hash Algorithm: sha256

md5: 7a1e0f635a9e45290cb24c8418d389d7

sha1: a8e948695bdbd85c5b848dc86fd3667e5ce14c07

sha256: 462ce30c9a62c1a966439549358edff6662fce832333382e12cc05519b18242f

sha512: ed2cd50ae1cfc1f8d6a364c26ed19085a57dc286722ee77a15aa061dcd94ec888e7365a79ac28048ba52ff71b3bd81bee9e13becb8b268703b95d669e9fa2faa

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 7711d77e42cb21cd24c6af106cebfe44204344af4adfc1e633895b5c6abdedce

## ☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_MEDIA_AUDIO	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_IMAGES	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
com.amazon.device.messaging.permission.RECEIVE	unknown	Unknown permission	Unknown permission from android reference
pt.ctt.outsystems.CTT.permission.RECEIVE_ADM_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
pt.ctt.outsystems.CTT.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

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.
com.sec.android.provider.badge.permission.READ	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	Show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.huawei.android.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference



FILE	DETAILS
------	---------



FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible Build.SERIAL check network operator name check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)

## BROWSABLE ACTIVITIES

ACTIVITY	INTENT
pt.ctt.outsystems.CTT.MainActivity	Schemes: pt.ctt.outsystems.ctt://, Hosts: appserver.ctt.pt,

## NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	warning	Base config is configured to trust system certificates.

## CERTIFICATE ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

## MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	<p>Broadcast Receiver (com.onesignal.ADMMessageHandler\$Receiver) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: com.amazon.device.messaging.permission.SEND [android:exported=true]</p>	warning	<p>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.</p>
4	<p>Broadcast Receiver (com.onesignal.GcmBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: com.google.android.c2dm.permission.SEND [android:exported=true]</p>	warning	<p>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.</p>
5	<p>Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: com.google.android.c2dm.permission.SEND [android:exported=true]</p>	warning	<p>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.</p>
6	<p>High Intent Priority (999) [android:priority]</p>	warning	<p>By setting an intent priority higher than another intent, the app effectively overrides other requests.</p>

# </> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	<a href="#">The App logs information. Sensitive information should never be logged.</a>	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/cookpad/puree/Puree.java com/cookpad/puree/internal/LogDumper.java com/cookpad/puree/internal/PureeVerboseRunnable.java com/cookpad/puree/storage/PureeSQLiteStorage.java com/cordova/launchstore/LaunchMobileStore.java com/journeyapps/barcodescanner/CameraPreview.java com/journeyapps/barcodescanner/CaptureManager.java com/journeyapps/barcodescanner/DecoderThread.java com/journeyapps/barcodescanner/camera/AutoFocusManager.java com/journeyapps/barcodescanner/camera/CameraConfigurationUtils.java com/journeyapps/barcodescanner/camera/CameraInstance.java com/journeyapps/barcodescanner/camera/CameraManager.java com/journeyapps/barcodescanner/camera/CenterCropStrategy.java com/journeyapps/barcodescanner/camera/FitCenterStrategy.java com/journeyapps/barcodescanner/camera/LegacyPreviewScalingStrategy.java com/journeyapps/barcodescanner/camera/PreviewScalingStrategy.java com/onesignal/AndroidSupportV4Compat.java com/onesignal/JobIntentService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/onesignal/jobinterceptor/Service.java com/onesignal/shortcutbadger/ShortcutBadger.java com/outsystems/imageeditor/view/ImageCropperView.java com/outsystems/plugins/applicationinfo/OSApplicationInfo.java com/outsystems/plugins/applicationinfo/OSApplicationInfoPlugin.java com/outsystems/plugins/oslogger/engines/puree/OSPureeBaseFilter.java com/outsystems/plugins/oslogger/engines/puree/OSPureeConsoleOutput.java com/outsystems/plugins/oslogger/helpers/OSWebViewCookieHandler.java com/outsystems/plugins/ossecurity/HttpClientCordovaPlugin.java io/sqlc/SQLiteAndroidDatabase.java io/sqlc/SQLiteConnectorDatabase.java io/sqlc/SQLitePlugin.java
2	<a href="#">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.</a>	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/cookpad/puree/storage/PureeSQLiteStorage.java com/onesignal/OneSignalDbHelper.java com/onesignal/outcomes/OSOutcomeTableProvider.java io/sqlc/SQLiteAndroidDatabase.java
3	<a href="#">MD5 is a weak hash known to have hash collisions.</a>	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/outsystems/plugins/oscache/cache/helpers/FileChecksum.java
4	<a href="#">App can read/write to External Storage. Any App can read data written to External Storage.</a>	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/outsystems/plugins/loader/clients/ChromeClient.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	<a href="#">Files may contain hardcoded sensitive information like usernames, passwords, keys etc.</a>	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/onesignal/NotificationBundleProcessor.java com/onesignal/OSInAppMessageController.java com/onesignal/OSInAppMessageLocationPrompt.java com/onesignal/OSInAppMessagePrompt.java com/onesignal/OneSignalNotificationManager.java com/onesignal/OneSignalRemoteParams.java
6	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	com/journeyapps/barcodescanner/CaptureManager.java

## NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	<a href="#">FCS_RBG_EXT.1.1</a>	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	<a href="#">FCS_STO_EXT.1.1</a>	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	<a href="#">FCS_CKM_EXT.1.1</a>	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
4	<a href="#">FDP_DEC_EXT.1.1</a>	Security Functional Requirements	Access to Platform Resources	The application has access to ['microphone', 'location', 'network connectivity', 'camera'].
5	<a href="#">FDP_DEC_EXT.1.2</a>	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	<a href="#">FDP_NET_EXT.1.1</a>	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	<a href="#">FDP_DAR_EXT.1.1</a>	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	<a href="#">FMT_MEC_EXT.1.1</a>	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	<a href="#">FTP_DIT_EXT.1.1</a>	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.
10	<a href="#">FCS_RBG_EXT.2.1</a> , <a href="#">FCS_RBG_EXT.2.2</a>	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	<a href="#">FCS_CKM.1.1(1)</a>	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
12	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.
13	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
14	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.
15	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.

## DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
journeyapps.com	ok	<b>IP:</b> 65.9.44.15 <b>Country:</b> United States of America <b>Region:</b> Washington <b>City:</b> Seattle <b>Latitude:</b> 47.606209 <b>Longitude:</b> -122.332069 <b>View:</b> <a href="#">Google Map</a>



DOMAIN	STATUS	GEOLOCATION
api.onesignal.com	ok	<b>IP:</b> 104.18.215.59 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>
play.google.com	ok	<b>IP:</b> 142.250.74.46 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
github.com	ok	<b>IP:</b> 140.82.121.4 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>

## TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	<a href="https://reports.exodus-privacy.eu.org/trackers/49">https://reports.exodus-privacy.eu.org/trackers/49</a>

TRACKER	CATEGORIES	URL
OneSignal		<a href="https://reports.exodus-privacy.eu.org/trackers/193">https://reports.exodus-privacy.eu.org/trackers/193</a>

## HARDCODED SECRETS

POSSIBLE SECRETS
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

## PLAYSTORE INFORMATION

**Title:** CTT - Correios de Portugal

**Score:** 0 **Installs:** 10,000+ **Price:** 0 **Android Version Support:** Business **Play Store URL:** [pt.ctt.outsystems.CTT](https://play.google.com/store/apps/details?id=pt.ctt.outsystems.CTT)

**Developer Details:** CTT-Correios de Portugal, S.A., CTT-Correios+de+Portugal,+S.A., None, None, informacao@ctt.pt,

**Release Date:** Oct 20, 2022 **Privacy Policy:** [Privacy link](#)

### Description:

In the CTT App you can manage your CTT and other operators' deliveries and shipments, pay tolls, take CTT stores digital tickets, among other solutions. App features: - Deliveries: manage and change express and mail orders with the chance of following CTT objects and other operators in real time. - Shipping: create express and mail shipments digitally, with the most convenient shipping and payment options. - Tolls: check your toll debts, pay with an ATM reference and subscribe online notifications. - Locky: choose your Locky that is most convenient to receive your orders. - Digital ticket: take a digital ticket to anticipate going to the CTT Store without having to take a ticket in person.

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.

© 2023 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).