ANDROID STATIC ANALYSIS REPORT

app_icon

RTO Challan (v12.5.1-25.10.22)

File Name:	E-CHALLAN-RTO.apk
Package Name:	com.zmh.wkjwqvogg
Scan Date:	Oct. 29, 2025, 3:40 p.m.

App Security Score: 42/100 (MEDIUM RISK)

Grade: B

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	ℹ INFO	✓ SECURE	HOTSPOT
5	17	2	1	1

FILE INFORMATION

File Name: E-CHALLAN-RTO.apk

Size: 14.93MB
MD5: 753876b01b6895c68ea4728422f0fc34
SHA1: 48c3e982ecadc113082ccd848e64b1243e80b8b6
SHA256: 888f6f88a85117e50a8d3c44e67a90132a514451474d67f832c58a3f6db9bcb5

APP INFORMATION

App Name: RTO Challan
Package Name: com.zmh.wkjwqvogg
Main Activity: pnw6gk.ccgy04
Target SDK: 28
Min SDK: 26
Max SDK:
Android Version Name: v12.5.1-25.10.22
Android Version Code: 1251

APP COMPONENTS

Activities: 8
Services: 8
Receivers: 7
Providers: 1
Exported Activities: 4
Exported Services: 1
Exported Receivers: 6
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: None
X.509 Subject: CN=rxyNeAvf
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2025-10-24 11:13:46+00:00
Valid To: 2035-10-22 11:13:46+00:00
Issuer: CN=rxyNeAvf
Serial Number: 0xb659a3dd7f60207e
Hash Algorithm: sha384
md5: 18e2c02e7b6ac7d8a2e4fcd3749ba867
sha1: f3de2dfaeec0778b31bc6dae383b6cfc21e32de6
sha256: 13ee993d27ebd8163b8c5fc7ced5841b7f56d3424c3c574eba08fdbae3d4d8b0
sha512: fbeb246b5360026e583395424f0a8e389f387b271539cd0f207145463d6f63bef2250b2dc4515416f35c85eb9dce293337fdcca0bca0fbd0668de643a4db0446
PublicKey Algorithm: rsa
Bit Size: 2048

Fingerprint: 9a70c286229a0eafedfdb061d001169a3d203123a6dfeb587c5c68334a2e42eb
Found 1 unique certificates

☰ 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.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.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.FOREGROUND_SERVICE_SPECIAL_USE	normal	enables special-use foreground services.	Allows a regular application to use Service.startForeground with the type "specialUse".
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
co.ec.cnsyn.codecatcher.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr><tr><td>Compiler</td><td>dexlib 2.x</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **1**

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

MANIFEST ANALYSIS

HIGH: **5** | WARNING: **13** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Activity (pnw6gk.ccgy04) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (28) of the app to 29 or higher to fix this issue at platform level.
4	Broadcast Receiver (com.zmh.wkjwqvogg.eAbfiNiH) is not Protected. [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.
5	Service (com.zmh.wkjwqvogg.eWtZTAlfORjhMVijR) 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.
6	Broadcast Receiver (com.zmh.wkjwqvogg.ebCMUgoC) is not Protected. [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.
7	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.
8	Activity (co.ec.cnsyn.codecatcher.MainActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (28) of the app to 29 or higher to fix this issue at platform level.
9	Activity (co.ec.cnsyn.codecatcher.MainActivity) 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.
10	Activity (co.ec.cnsyn.codecatcher.ActionActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (28) of the app to 29 or higher to fix this issue at platform level.
11	Activity (co.ec.cnsyn.codecatcher.ActionActivity) 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.
12	Activity (co.ec.cnsyn.codecatcher.DebugActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (28) of the app to 29 or higher to fix this issue at platform level.

NO	ISSUE	SEVERITY	DESCRIPTION
13	Activity (co.ec.cnsyn.codecatcher.DebugActivity) 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.
14	Broadcast Receiver (co.ec.cnsyn.codecatcher.sms.SmsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BROADCAST_SMS [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.
15	Broadcast Receiver (co.ec.cnsyn.codecatcher.sms.BootReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.RECEIVE_BOOT_COMPLETED [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.
16	Activity (androidx.compose.ui.tooling.PreviewActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (28) of the app to 29 or higher to fix this issue at platform level.
17	Activity (androidx.compose.ui.tooling.PreviewActivity) 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.
18	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 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: **0** | WARNING: **3** | INFO: **2** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	A/J.java C/C0034l.java D1/f.java E1/a.java G0/z.java I1/C0211g.java I1/F.java L/C0.java N0/v.java S0/f.java S0/n.java S1/a.java T0/a.java Z/e.java a/AbstractC0394a.java d1/AbstractC0519f.java d1/C0521h.java d1/C0522i.java e/d.java e1/AbstractC0535a.java f1/d.java g1/b.java j1/AbstractC0704F.java j1/AbstractC0710L.java j1/AbstractC0733l.java j1/AbstractC0742u.java j1/C0705G.java m0/C0904a.java o1/AbstractC0962d.java p0/AbstractC1028c.java v/C1129e.java v1/C1164A.java v1/C1187l.java y/C1309Q.java y0/C1347D.java y0/r.java y1/AbstractC1406d.java z1/i.java z1/j.java
2	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	S1/i.java y0/V.java y2/a.java y2/b.java z2/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	D1/h.java b2/C0466b.java co/ec/cnsyn/codecatcher/ActionActivity.java y0/C1366h.java
4	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	I/C0174s0.java L/C0297f0.java L0/F.java T2/Q.java
5	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	D1/b.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	I1/C0211g.java S0/f.java d1/C0520g.java e1/AbstractC0535a.java o1/AbstractC0962d.java y1/AbstractC1406d.java y1/C1403a.java y1/i.java
00056	Modify voice volume	control	b2/C0471g.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	C/s0.java I1/C0213i.java v1/C1164A.java y0/Y.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	C/s0.java l1/C0213i.java
00036	Get resource file from res/raw directory	reflection	l1/C0213i.java
00193	Send a SMS message	sms	b2/C0466b.java
00028	Read file from assets directory	file	co/ec/cnsyn/codecatcher/ba5sou3sioz1kaiD.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.REQUEST_INSTALL_PACKAGES, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	4/44	android.permission.FOREGROUND_SERVICE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, com.google.android.c2dm.permission.RECEIVE, android.permission.MODIFY_AUDIO_SETTINGS

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

DOMAIN	STATUS	GEOLOCATION
goo.gle	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.251.38.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
fonts.gstatic.com	ok	**IP:** 142.251.38.67 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
youtrack.jetbrains.com	ok	**IP:** 63.35.30.167 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

✉ EMAILS

EMAIL	FILE
de-catcher-translate@proxiedmail.com	C/s0.java

HARDCODED SECRETS

POSSIBLE SECRETS
2486b7807e76ac15ef62438eff3e2f97
77125838e78926987debd3e76ea8ebd5
ecwpcv70jcibydeqfhqqejz8lx34ey0t8fyvgbsxtrexltbf03lprqdzahlcoffu

SCAN LOGS

Timestamp	Event	Error
2025-10-29 16:00:32	Generating Hashes	OK
2025-10-29 16:00:32	Extracting APK	OK
2025-10-29 16:00:32	Unzipping	OK
2025-10-29 16:00:32	Parsing APK with androguard	OK
2025-10-29 16:00:33	Extracting APK features using aapt/aapt2	OK
2025-10-29 16:00:33	Getting Hardcoded Certificates/Keystores	OK
2025-10-29 16:00:33	Parsing AndroidManifest.xml	OK

2025-10-29 16:00:33	Extracting Manifest Data	OK
2025-10-29 16:00:33	Manifest Analysis Started	OK
2025-10-29 16:00:33	Performing Static Analysis on: RTO Challan (com.zmh.wkjwqvogg)	OK
2025-10-29 16:00:34	Fetching Details from Play Store: com.zmh.wkjwqvogg	OK
2025-10-29 16:00:34	Checking for Malware Permissions	OK
2025-10-29 16:00:34	Fetching icon path	OK
2025-10-29 16:00:34	Library Binary Analysis Started	OK
2025-10-29 16:00:34	Reading Code Signing Certificate	OK
2025-10-29 16:00:34	Failed to get signature versions with apksigner	CalledProcessError(1, ['/jdk-22.0.2/bin/java', '-Xmx1024M', '-Djava.library.path=', '-jar', '/home/mobsf/Mobile-Security-Framework-MobSF/mobsf/StaticAnalyzer/tools/apksigner.jar', 'verify', '--verbose', '/home/mobsf/.MobSF/uploads/753876b01b6895c68ea4728422f0fc34/753876b01b6895c68ea4728422f0fc34.apk'])
2025-10-29 16:00:34	Running APKiD 3.0.0	OK
2025-10-29 16:00:36	Detecting Trackers	OK
2025-10-29 16:00:37	Decompiling APK to Java with JADX	OK
2025-10-29 16:00:39	Decompiling with JADX failed, attempting on all DEX files	OK
2025-10-29 16:00:39	Decompiling classes.dex with JADX	OK

2025-10-29 16:00:59	Converting DEX to Smali	OK
2025-10-29 16:00:59	Code Analysis Started on - java_source	OK
2025-10-29 16:01:00	Android SBOM Analysis Completed	OK
2025-10-29 16:01:36	Android SAST Completed	OK
2025-10-29 16:01:36	Android API Analysis Started	OK
2025-10-29 16:01:38	Android API Analysis Completed	OK
2025-10-29 16:01:39	Android Permission Mapping Started	OK
2025-10-29 16:01:42	Android Permission Mapping Completed	OK
2025-10-29 16:01:42	Android Behaviour Analysis Started	OK
2025-10-29 16:02:15	Android Behaviour Analysis Completed	OK
2025-10-29 16:02:15	Extracting Emails and URLs from Source Code	OK
2025-10-29 16:02:18	Email and URL Extraction Completed	OK
2025-10-29 16:02:18	Extracting String data from Code	OK
2025-10-29 16:02:18	Extracting String values and entropies from Code	OK

2025-10-29 16:02:19	Performing Malware check on extracted domains	OK
2025-10-29 16:02:20	Saving to Database	OK

Report Generated by - MobSF v4.4.3

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.