ANDROID STATIC ANALYSIS REPORT

app_icon

PM YOJANA (v10.2-25.9.8)

File Name:	PM_KISAN_YOJNA_M15.apk
Package Name:	com.uqbmygi.zefsgzr
Scan Date:	Oct. 16, 2025, 2:26 a.m.

App Security Score: 43/100 (MEDIUM RISK)

Grade: B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	9	1	1	1

FILE INFORMATION

File Name: PM_KISAN_YOJNA_M15.apk
Size: 9.37MB
MD5: 97ce40ff2ed9d63b98683313d80fc7ff
SHA1: f6e3d685caa2a4f84612d72126ce703a859b5cd1
SHA256: ac1b68c0284f698a2b24d6bd9486d059d25acd7b968e85124c602a0d87858d23

APP INFORMATION

App Name: PM YOJANA
Package Name: com.uqbmygi.zefsgzr
Main Activity: pb09hj.cjqq4g
Target SDK: 28
Min SDK: 24
Max SDK:
Android Version Name: v10.2-25.9.8
Android Version Code: 8

APP COMPONENTS

Activities: 4
Services: 6
Receivers: 4
Providers: 0
Exported Activities: 0
Exported Services: 1
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: None
X.509 Subject: CN=DgBrdCGp
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2025-09-08 13:17:17+00:00
Valid To: 2035-09-06 13:17:17+00:00
Issuer: CN=DgBrdCGp
Serial Number: 0x5960f54009a551e
Hash Algorithm: sha384
md5: 8dde330e149ac70d6fd395c880bc9351
sha1: 9a7d35a4b9bb098a1e5f2e3eaf5004b80425977d
sha256: ad14c464d28b9ee3fe03412a6d78ffd621d46f6366bb2adc53733a1d3115db8e

sha512: fc484fc143a1db70d962b07ce87c54c6cf77568e4025a4867dfd6ea5314360add3f6a488e0df9f3d90ccff0e280c765d90e36178ebf1485b5cc3bb2687f36f70
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 05ac2a629f1acf719cc9da0e4b06d995a088dfae7a354af088662fcfee02c80d
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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Compiler — DETAILS: dexlib 2.x
classes2.dex	FINDINGS: Compiler — DETAILS: dexlib 2.x

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: 3 | WARNING: 4 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	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.
3	Activity (pb09hj.cjqq4g) 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.uqbmygi.zefsgzr.ehePxWPjkmibT) 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.uqbmygi.zefsgzr.ejfQiOaDqUDVoUnd) 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.uqbmygi.zefsgzr.eLjwqAVjDYV) 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.

</> CODE ANALYSIS

HIGH: **0** | WARNING: **5** | INFO: **1** | 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	com/badlogic/gdx/backends/android/AndroidApplication.java com/badlogic/gdx/backends/android/AndroidLiveWallpaper.java com/badlogic/gdx/backends/android/AndroidLiveWallpaperService.java com/badlogic/gdx/backends/android/AndroidOnscreenKeyboard.java com/badlogic/gdx/backends/android/surfaceview/EGLLogWrapper.java com/badlogic/gdx/backends/android/surfaceview/GLBaseSurfaceView.java com/badlogic/gdx/backends/android/surfaceview/GLLogWrapper.java com/badlogic/gdx/backends/android/surfaceview/GLSurfaceView20.java com/badlogic/gdx/backends/android/surfaceview/GLSurfaceView20LW.java com/badlogic/gdx/backends/android/surfaceview/GLSurfaceViewCupcake.java com/badlogic/gdx/backends/android/surfaceview/GdxEglConfigChooser.java com/badlogic/gdx/math/Intersector.java com/badlogic/gdx/utils/GdxNativesLoader.java com/badlogic/gdx/utils/GwtModuleGenerator.java com/badlogic/gdx/utils/JsonReader.java org/projectmaxs/shared/global/jul/JULHandler.java org/projectmaxs/shared/global/util/Log.java org/projectmaxs/shared/module/MAXSModuleIntentService.java org/projectmaxs/shared/module/MAXSModuleReceiver.java
2	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	org/projectmaxs/shared/global/StatusInformation.java org/projectmaxs/shared/mainmodule/MAXSContentProviderContract.java
3	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/badlogic/gdx/backends/android/AndroidFiles.java com/badlogic/gdx/files/FileHandle.java org/projectmaxs/shared/global/GlobalConstants.java
4	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/badlogic/gdx/files/FileHandle.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	org/projectmaxs/module/smssend/database/SMSSendDatabase.java
6	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/badlogic/gdx/math/MathUtils.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/liblnhjntev.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/liblnhjntev.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memmove_chk', '__strlen_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00035	Query the list of the installed packages	reflection	org/projectmaxs/shared/global/util/PackageManagerUtil.java
00028	Read file from assets directory	file	com/badlogic/gdx/backends/android/AndroidFileHandle.java
00022	Open a file from given absolute path of the file	file	com/badlogic/gdx/utils/GdxNativesLoader.java com/badlogic/gdx/utils/SharedLibraryLoader.java org/projectmaxs/shared/global/FilereadUtil.java
00162	Create InetSocketAddress object and connecting to it	socket	com/badlogic/gdx/backends/android/AndroidSocket.java
00163	Create new Socket and connecting to it	socket	com/badlogic/gdx/backends/android/AndroidSocket.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/badlogic/gdx/files/FileHandle.java
00012	Read data and put it into a buffer stream	file	com/badlogic/gdx/files/FileHandle.java
00192	Get messages in the SMS inbox	sms	org/projectmaxs/shared/global/FilereadUtil.java org/projectmaxs/shared/module/ContactUtil.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	org/projectmaxs/shared/module/ContactUtil.java
00187	Query a URI and check the result	collection sms calllog calendar	org/projectmaxs/shared/module/ContactUtil.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	org/projectmaxs/shared/module/ContactUtil.java
00040	Send SMS	sms	org/projectmaxs/module/smssend/commands/AbstractSmsSendCommand.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/badlogic/gdx/backends/android/AndroidNet.java org/projectmaxs/shared/global/FilereadUtil.java org/projectmaxs/shared/global/util/DialogUtil.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	3/44	android.permission.FOREGROUND_SERVICE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, com.google.android.c2dm.permission.RECEIVE

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
www.openstreetmap.org	ok	**IP:** 104.21.88.66 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
projectmaxs.org	ok	**IP:** 5.45.100.158 **Country:** Germany **Region:** Baden-Wurttemberg **City:** Karlsruhe **Latitude:** 49.004719 **Longitude:** 8.385830 **View:** Google Map
bitbucket.org	ok	**IP:** 13.200.41.134 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

SCAN LOGS

Timestamp	Event	Error
2025-10-16 02:26:24	Generating Hashes	OK
2025-10-16 02:26:24	Extracting APK	OK
2025-10-16 02:26:24	Unzipping	OK
2025-10-16 02:26:24	Parsing APK with androguard	OK
2025-10-16 02:26:24	Extracting APK features using aapt/aapt2	OK
2025-10-16 02:26:24	Getting Hardcoded Certificates/Keystores	OK
2025-10-16 02:26:25	Parsing AndroidManifest.xml	OK
2025-10-16 02:26:25	Extracting Manifest Data	OK
2025-10-16 02:26:25	Manifest Analysis Started	OK
2025-10-16 02:26:25	Performing Static Analysis on: PM YOJANA (com.uqbmygi.zefsgzr)	OK
2025-10-16 02:26:26	Fetching Details from Play Store: com.uqbmygi.zefsgzr	OK
2025-10-16 02:26:27	Checking for Malware Permissions	OK
2025-10-16 02:26:27	Fetching icon path	OK

2025-10-16 02:26:27	Library Binary Analysis Started	OK
2025-10-16 02:26:27	Analyzing lib/armeabi-v7a/liblnhjntev.so	OK
2025-10-16 02:26:27	Analyzing lib/arm64-v8a/liblnhjntev.so	OK
2025-10-16 02:26:27	Reading Code Signing Certificate	OK
2025-10-16 02:26:27	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/97ce40ff2ed9d63b98683313d80fc7ff/97ce40ff2ed9d63b98683313d80fc7ff.apk'])
2025-10-16 02:26:27	Running APKiD 3.0.0	OK
2025-10-16 02:26:29	Detecting Trackers	OK
2025-10-16 02:26:30	Decompiling APK to Java with JADX	OK
2025-10-16 02:26:31	Decompiling with JADX failed, attempting on all DEX files	OK
2025-10-16 02:26:31	Decompiling classes.dex with JADX	OK
2025-10-16 02:26:35	Decompiling classes2.dex with JADX	OK
2025-10-16 02:26:36	Converting DEX to Smali	OK
2025-10-16 02:26:36	Code Analysis Started on - java_source	OK

2025-10-16 02:26:37	Android SBOM Analysis Completed	OK
2025-10-16 02:26:38	Android SAST Completed	OK
2025-10-16 02:26:38	Android API Analysis Started	OK
2025-10-16 02:26:38	Android API Analysis Completed	OK
2025-10-16 02:26:39	Android Permission Mapping Started	OK
2025-10-16 02:26:39	Android Permission Mapping Completed	OK
2025-10-16 02:26:39	Android Behaviour Analysis Started	OK
2025-10-16 02:26:40	Android Behaviour Analysis Completed	OK
2025-10-16 02:26:40	Extracting Emails and URLs from Source Code	OK
2025-10-16 02:26:41	Email and URL Extraction Completed	OK
2025-10-16 02:26:41	Extracting String data from SO	OK
2025-10-16 02:26:41	Extracting String data from Code	OK
2025-10-16 02:26:41	Extracting String values and entropies from Code	OK
2025-10-16 02:26:41	Performing Malware check on extracted domains	OK

2025-10-16 02:26:43	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.