ANDROID STATIC ANALYSIS REPORT

PM-KISAN List 2024-25 (1.0)

File Name:	PM_Kisan_list_2024_-_2025.apk
Package Name:	com.example.myapplication
Scan Date:	March 15, 2025, 4:04 p.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
6	15	1	3	2

FILE INFORMATION

File Name: PM_Kisan_list_2024_-_2025.apk
Size: 13.84MB
MD5: 81b3c8d299ee772c4ca62695cdbe9f47
SHA1: 7094d7798389205740ea9df4a09107d92636dec9
SHA256: a89565a1a10363506df1248e6c8a2ae73d59446ffbf1819478eac449abfce08b

APP INFORMATION

App Name: PM-KISAN List 2024-25
Package Name: com.example.myapplication
Main Activity: com.ZXOo.fMJItBt.MainActivity
Target SDK: 28
Min SDK: 23
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 3

Services: 7

Receivers: 5

Providers: 2

Exported Activities: 1

Exported Services: 1

Exported Receivers: 4

Exported Providers: 0

✹ CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: CN=sEygqTtY
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2025-03-13 13:13:28+00:00
Valid To: 2035-03-11 13:13:28+00:00
Issuer: CN=sEygqTtY
Serial Number: 0x3e1dec0d5b6172c1
Hash Algorithm: sha384
md5: b22493a2ce698832cbaf4d668731352b
sha1: 977b112e04a19e7c4ef8cfe1751f7c0a9c49cb1a
sha256: 9f6ad7d20ba4262aef2e5b645239db3958d5bebbb7528655521c0c71db0e814e
sha512: 5c85aab68087d63355925d7dd528a7c2baf38866bae2eb33302d8daa8ec7756540216f6629311d704879fc35e93109c755c4cd04f0a6c18e434a96b9becad02b
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: d4ecc2ea5f27c2cb92e3795ba6e8adb5d2fa1846480fd66c42c3a789b40a52ae
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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
com.example.myapplication.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

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

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

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.

MANIFEST ANALYSIS

HIGH: **4** | WARNING: **7** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	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	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.ZXOo.fMJItBt.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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Activity (com.ZXOo.fMJItBt.MainAliasActivity) 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.
6	Activity-Alias (com.ZXOo.fMJItBt.MainAliasActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias 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.ZXOo.fMJItBt.InstallReceiver) 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.
8	Service (com.ZXOo.fMJItBt.LocalVPNService) 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.
9	Broadcast Receiver (com.example.fcmexpr.keepalive.KeepAliveReceiver) 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.
10	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.

NO	ISSUE	SEVERITY	DESCRIPTION
11	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: **2** | WARNING: **6** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Aebu8yohvea8/Eikuh5Phaeth.java Aebu8yohvea8/Ohah9Nai3tha.java Aebu8yohvea8/ahz5eechei8U.java Aebu8yohvea8/baexaike8KuV.java Aebu8yohvea8/doonge7ooYoe.java Aebu8yohvea8/eewoo9thaiCe.java Aebu8yohvea8/eyei9eigh3Ie.java Aebu8yohvea8/ieseir3Choge.java Aebu8yohvea8/keiL1EiShomu.java Aebu8yohvea8/lo8zieZoeseb.java Aebu8yohvea8/zoo3eifoe3Ae.java Aena7ahweute/thooCoci9zae.java Aicohm8ieYoo/thooCoci9zae.java Do5Ierepupup/ieseir3Choge.java Eikuh5Phaeth/ahthoK6usais.java Eikuh5Phaeth/keiL1EiShomu.java Eikuh5Phaeth/ruwiepo7ooVu.java IPh5ahNg5Ooj/thooCoci9zae.java Id9uvaegh4ai/mi5Iecheimie.java Ohgahseiw0ni/ieseir3Choge.java Ugh8Ookozohy/AeJiPo4of6Sh.java Ugh8Ookozohy/Iah0aiP1ki6y.java

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	Ugh8Ookozony/Jah0aiP1ki6y.java Xe6mangaekai/IengaiSahh8H.java Xe6mangaekai/Ochoob6Ahvi2.java Xe6mangaekai/eyei9eigh3le.java Xe6mangaekai/kah6Uo2ooji4.java Xe6mangaekai/keiL1EiShomu.java Xe6mangaekai/ohthie9thieG.java Xe6mangaekai/ruNgecai1pae.java Xe6mangaekai/thooCoci9zae.java Xix0Vei5vo3j/thooCoci9zae.java aech7ohPhooh/Jah0aiP1ki6y.java aech7ohPhooh/ko7aiFeiqu3s.java aech7ohPhooh/laej2zeez5Ja.java aech7ohPhooh/mi5Iecheimie.java aech7ohPhooh/ohthie9thieG.java aech7ohPhooh/ruNgecai1pae.java ahSixio7zefo/ieseir3Choge.java ahk3OhSh9Ree/keiL1EiShomu.java com/ZXOo/fMJItBt/FakeActivity.java com/ZXOo/fMJItBt/InstallReceiver.java com/ZXOo/fMJItBt/LocalVPNService.java com/ZXOo/fMJItBt/MainActivity.java com/example/fcmexpr/keepalive/FirebaseMessagingKeepAliveService.java com/example/fcmexpr/keepalive/KeepAliveReceiver.java com/example/fcmexpr/keepalive/KeepAliveServiceMediaPlayback.java doonge7ooYoe/ruNgecai1pae.java eabiePho2iu8/Aicohm8ieYoo.java eabiePho2iu8/Eipeibai2Aa0.java eabiePho2iu8/IengaiSahh8H.java eabiePho2iu8/Meu0ophaeng1.java eabiePho2iu8/Naid2tee7aeb.java eabiePho2iu8/Ohgahseiw0ni.java eabiePho2iu8/ahk3OhSh9Ree.java eabiePho2iu8/eetheKaevie8.java eabiePho2iu8/ieheiQu9sho5.java eabiePho2iu8/iev8ainaiLae.java eabiePho2iu8/io4laQuei7sa.java eabiePho2iu8/maSie9ief8Ae.java eabiePho2iu8/mi3Ozool1oa4.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				eabiePho2iu8/ohv5Shie7AeZ.java eabiePho2iu8/ohx8eem3Ahph.java eabiePho2iu8/ooJahquoo9ei.java eabiePho2iu8/ruwiepo7ooVu.java eabiePho2iu8/soiNgemai6Ie.java eabiePho2iu8/soo9aeJ3kahb.java eetheKaevie8/ahthoK6usais.java eetheKaevie8/ko7aiFeiqu3s.java eetheKaevie8/niah0Shohtha.java eetheKaevie8/oYe2ma2she1j.java eetheKaevie8/ruNgecai1pae.java eewoo9thaiCe/keiL1EiShomu.java eik1oetahvuF/HaeYeFaep1if.java eik1oetahvuF/Ochoob6Ahvi2.java eik1oetahvuF/ahz5eechei8U.java eik1oetahvuF/kuedujio7Aev.java eik1oetahvuF/ohthie9thieG.java esohshee3Pau/kuedujio7Aev.java eyei9eigh3Ie/IengaiSahh8H.java eyei9eigh3Ie/ahz5eechei8U.java eyei9eigh3Ie/kah6Uo2ooji4.java eyei9eigh3Ie/ohthie9thieG.java ieph3Uteimah/Jah0aiP1ki6y.java niah0Shohtha/Idohhaimaes0.java niah0Shohtha/Ochoob6Ahvi2.java niah0Shohtha/kah6Uo2ooji4.java niah0Shohtha/lo8zieZoeseb.java niah0Shohtha/oYe2ma2she1j.java niah0Shohtha/ohthie9thieG.java niah0Shohtha/soiNgemai6Ie.java oYe2ma2she1j/ieheiQu9sho5.java oYe2ma2she1j/keiL1EiShomu.java oYe2ma2she1j/niah0Shohtha.java ohBoophood9o/kuedujio7Aev.java ohx8eem3Ahph/eetheKaevie8.java ohx8eem3Ahph/kuedujio7Aev.java ohx8eem3Ahph/niah0Shohtha.java ohx8eem3Ahph/ruwiepo7ooVu.java org/conscrypt/Platform.java org/conscrypt/ct/CTVerifier.java rojaiZ9aeRee/ahthoK6usais.java sieChi1iehoo/thooCoci9zae.java soiNgemai6Ie/thooCoci9zae.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				soiNgemaiole/thooCoci9zae.java waita4vool1K/keiL1EiShomu.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	Aevahngah0ah/aeTh5ATha5te.java org/conscrypt/OpenSSLECKeyFactory.java org/conscrypt/OpenSSLRSAKeyFactory.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/ZXOo/fMJltBt/LocalVPNService.java org/conscrypt/CertificatePriorityComparator.java org/conscrypt/ChainStrengthAnalyzer.java org/conscrypt/EvpMdRef.java org/conscrypt/OAEPParameters.java org/conscrypt/OidData.java org/conscrypt/OpenSSLCipherRSA.java org/conscrypt/OpenSSLECGroupContext.java org/conscrypt/OpenSSLProvider.java org/conscrypt/OpenSSLSignature.java org/conscrypt/TrustManagerImpl.java org/conscrypt/ct/CTConstants.java tierieCoh4wi/thooCoci9zae.java
4	[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	Aevahngah0ah/IengaiSahh8H.java Aevahngah0ah/Vaig0nohza7i.java Aevahngah0ah/Wee3zai1phei.java Aevahngah0ah/mi3Ozool1oa4.java Aevahngah0ah/rahCagav5nie.java cie5Echaet0o/ohv5Shie7AeZ.java uc6lec4eomim/niah0Shohtha.java uc6lec4eomim/ruNgecai1pae.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	Xix0Vei5vo3j/thooCoci9zae.java org/conscrypt/Conscrypt.java org/conscrypt/DefaultSSLContextImpl.java org/conscrypt/SSLParametersImpl.java
6	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	zoo3eifoe3Ae/ieseir3Choge.java
7	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	Aena7ahweute/thooCoci9zae.java eabiePho2iu8/IengaiSahh8H.java zoo3eifoe3Ae/ieseir3Choge.java
8	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	Naid2tee7aeb/HaeYeFaep1if.java Naid2tee7aeb/zoo3eifoe3Ae.java
9	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
10	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	Aena7ahweute/keiL1EiShomu.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libconscrypt_jni.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.	False warning The binary 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. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libconscrypt_jni.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', '__strchr_chk', '__memset_chk', '__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	Xix0Vei5vo3j/thooCoci9zae.java ohx8eem3Ahph/ruwiepo7ooVu.java soo9aeJ3kahb/ieheiQu9sho5.java waita4vool1K/keiL1EiShomu.java
00089	Connect to a URL and receive input stream from the server	command network	Xix0Vei5vo3j/thooCoci9zae.java ohx8eem3Ahph/ruwiepo7ooVu.java soo9aeJ3kahb/ieheiQu9sho5.java waita4vool1K/keiL1EiShomu.java
00109	Connect to a URL and get the response code	network command	Xix0Vei5vo3j/thooCoci9zae.java ohx8eem3Ahph/ruwiepo7ooVu.java soo9aeJ3kahb/ieheiQu9sho5.java waita4vool1K/keiL1EiShomu.java
00091	Retrieve data from broadcast	collection	eabiePho2iu8/ahk3OhSh9Ree.java
00163	Create new Socket and connecting to it	socket	org/conscrypt/AbstractConscryptSocket.java org/conscrypt/KitKatPlatformOpenSSLSocketImplAdapter.java org/conscrypt/PreKitKatPlatformOpenSSLSocketImplAdapter.java
00013	Read file and put it into a stream	file	Aena7ahweute/keiL1EiShomu.java eetheKaevie8/ko7aiFeiqu3s.java eetheKaevie8/oYe2ma2she1j.java org/conscrypt/DefaultSSLContextImpl.java org/conscrypt/FileClientSessionCache.java org/conscrypt/KeyManagerFactoryImpl.java zoo3eifoe3Ae/ieseir3Choge.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	aech7ohPhooh/niah0Shohtha.java com/ZXOo/fMJItBt/FakeActivity.java com/example/fcmexpr/keepalive/KeepAliveServiceMediaPlayback.java eabiePho2iu8/ieheiQu9sho5.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	aech7ohPhooh/niah0Shohtha.java eabiePho2iu8/ieheiQu9sho5.java
00036	Get resource file from res/raw directory	reflection	aech7ohPhooh/niah0Shohtha.java eabiePho2iu8/ieheiQu9sho5.java
00162	Create InetSocketAddress object and connecting to it	socket	org/conscrypt/AbstractConscryptSocket.java
00022	Open a file from given absolute path of the file	file	eewoo9thaiCe/keiL1EiShomu.java ohx8eem3Ahph/niah0Shohtha.java
00028	Read file from assets directory	file	eewoo9thaiCe/keiL1EiShomu.java
00012	Read data and put it into a buffer stream	file	org/conscrypt/DefaultSSLContextImpl.java
00072	Write HTTP input stream into a file	command network file	ohx8eem3Ahph/ruwiepo7ooVu.java
00030	Connect to the remote server through the given URL	network	ohx8eem3Ahph/ruwiepo7ooVu.java
00094	Connect to a URL and read data from it	command network	ohx8eem3Ahph/ruwiepo7ooVu.java
00108	Read the input stream from given URL	network command	ohx8eem3Ahph/ruwiepo7ooVu.java
00014	Read file into a stream and put it into a JSON object	file	Aena7ahweute/keiL1EiShomu.java

RULE ID	BEHAVIOUR	LABEL	FILES
00161	Perform accessibility service action on accessibility node info	accessibility service	Idohhaimaes0/rojaiZ9aeRee.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	Idohhaimaes0/rojaiZ9aeRee.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/652224930385/namespaces/firebase:fetch?key=AIzaSyBi7EVzF-1BG3A_JkmtjZPJkPhsYu7ncAM. This is indicated by the response: {'state': 'NO_TEMPLATE'}

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	2/44	android.permission.FOREGROUND_SERVICE, 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
uasecurity.org	ok	**IP:** 162.250.189.197 **Country:** Canada **Region:** Quebec **City:** Saint-Laurent **Latitude:** 45.497772 **Longitude:** -73.679916 **View:** Google Map
firebase.google.com	ok	**IP:** 216.58.210.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
raw.githubusercontent.com	ok	**IP:** 185.199.110.133 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
api.uasecurity.org	ok	**IP:** 185.200.64.67 **Country:** Germany **Region:** Bayern **City:** Kreuzstrasse **Latitude:** 47.778660 **Longitude:** 11.722730 **View:** Google Map
play.google.com	ok	**IP:** 216.58.210.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
accessor.pages.dev	ok	**IP:** 104.21.32.1 **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.

EMAILS

EMAIL	FILE
u0013android@android.com u0013android@android.com0	aech7ohPhooh/aac1eTaexee6.java
appro@openssl.org	lib/arm64-v8a/libconscrypt_jni.so

HARDCODED SECRETS

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyBi7EVzF-1BG3A_JkmtjZPJkPhsYu7ncAM"
"google_api_key" : "AIzaSyBi7EVzF-1BG3A_JkmtjZPJkPhsYu7ncAM"

POSSIBLE SECRETS
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
b70e0cbd6bb4bf7f321390b94a03c1d356c21122343280d6115c1d21
b4050a850c04b3abf54132565044b0b7d7bfd8ba270b39432355ffb4
51953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
bd376388b5f723fb4c22dfe6cd4375a05a07476444d5819985007e34
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
44DhRjPJrQeNDqomajQjBvdD39UiQvoeh67ABYSWMZWEWKCB3Tzhvtw2jB9KC3UARF1gsBuhvEoNEd2qSDz76BYEPYNuPKD
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

SCAN LOGS

Timestamp	Event	Error

2025-03-15 16:04:04	Generating Hashes	OK
2025-03-15 16:04:04	Extracting APK	OK
2025-03-15 16:04:04	Unzipping	OK
2025-03-15 16:04:05	Parsing APK with androguard	OK
2025-03-15 16:04:05	Extracting APK features using aapt/aapt2	OK
2025-03-15 16:04:05	Getting Hardcoded Certificates/Keystores	OK
2025-03-15 16:04:06	Parsing AndroidManifest.xml	OK
2025-03-15 16:04:06	Extracting Manifest Data	OK
2025-03-15 16:04:06	Manifest Analysis Started	OK
2025-03-15 16:04:06	Performing Static Analysis on: PM-KISAN List 2024-25 (com.example.myapplication)	OK
2025-03-15 16:04:06	Fetching Details from Play Store: com.example.myapplication	OK

2025-03-15 16:04:06	Checking for Malware Permissions	OK
2025-03-15 16:04:06	Fetching icon path	OK
2025-03-15 16:04:06	Library Binary Analysis Started	OK
2025-03-15 16:04:06	Analyzing lib/armeabi-v7a/libconscrypt_jni.so	OK
2025-03-15 16:04:06	Analyzing lib/arm64-v8a/libconscrypt_jni.so	OK
2025-03-15 16:04:06	Reading Code Signing Certificate	OK
2025-03-15 16:04:08	Running APKiD 2.1.5	OK
2025-03-15 16:04:10	Detecting Trackers	OK
2025-03-15 16:04:11	Decompiling APK to Java with JADX	OK
2025-03-15 16:04:15	Decompiling with JADX failed, attempting on all DEX files	OK
2025-03-15 16:04:15	Decompiling classes.dex with JADX	OK

2025-03-15 16:04:34	Converting DEX to Smali	OK
2025-03-15 16:04:34	Code Analysis Started on - java_source	OK
2025-03-15 16:04:35	Android SBOM Analysis Completed	OK
2025-03-15 16:05:08	Android SAST Completed	OK
2025-03-15 16:05:08	Android API Analysis Started	OK
2025-03-15 16:05:11	Android API Analysis Completed	OK
2025-03-15 16:05:11	Android Permission Mapping Started	OK
2025-03-15 16:05:13	Android Permission Mapping Completed	OK
2025-03-15 16:05:14	Android Behaviour Analysis Started	OK
2025-03-15 16:05:16	Android Behaviour Analysis Completed	OK
2025-03-15 16:05:16	Extracting Emails and URLs from Source Code	OK

2025-03-15 16:05:17	Email and URL Extraction Completed	OK
2025-03-15 16:05:17	Extracting String data from APK	OK
2025-03-15 16:05:17	Extracting String data from SO	OK
2025-03-15 16:05:17	Extracting String data from Code	OK
2025-03-15 16:05:17	Extracting String values and entropies from Code	OK
2025-03-15 16:05:18	Performing Malware check on extracted domains	OK
2025-03-15 16:05:20	Saving to Database	OK

Report Generated by - MobSF v4.3.1

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.