



ANDROID STATIC ANALYSIS REPORT



 PulsePoint (4.20.1)

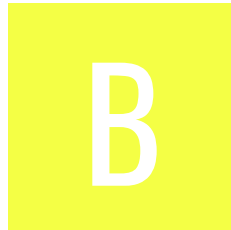
File Name: mobi.firedepartment_6122.apk

Package Name: mobi.firedepartment

Scan Date: Sept. 1, 2025, 2:34 p.m.






App Security Score: 50/100 (MEDIUM RISK)

Grade:



Trackers Detection: 2/432

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
2	47	3	2	1

FILE INFORMATION

File Name: mobi.firedepartment_6122.apk

Size: 30.8MB

MD5: e5f97f6dce976c0d1dbb58ecbdd8747d

SHA1: 453096f8be53c235273cadb5c037c29ad27cf032

SHA256: 3b54bfc7861704750e49e98de30b7bc7a8a4f9138c650abb14d5d7d8efdf80ca

APP INFORMATION

App Name: PulsePoint

Package Name: mobi.firedepartment

Main Activity: mobi.firedepartment.ui.views.splashscreen.SplashScreenActivity

Target SDK: 34

Min SDK: 28

Max SDK:

Android Version Name: 4.20.1

Android Version Code: 6122

APP COMPONENTS

Activities: 40

Services: 13

Receivers: 6

Providers: 2

Exported Activities: 38

Exported Services: 2

Exported Receivers: 3

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: False

v2 signature: False

v3 signature: True

v4 signature: False

X.509 Subject: C=US, ST=CA, L=San Ramon, O=PulsePoint Foundation, OU=Android, CN=Rob Byrne

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2011-11-29 20:23:16+00:00

Valid To: 2039-04-16 20:23:16+00:00

Issuer: C=US, ST=CA, L=San Ramon, O=PulsePoint Foundation, OU=Android, CN=Rob Byrne

Serial Number: 0x4ed53f34

Hash Algorithm: sha1

md5: 4d202132f67a498516bf518dd1cd58ff

sha1: 8d2211f4c24156fb2535d4f6d5364ce21625d2b8

sha256: 97559821f1147b3258a0718e6c53db868a3aceaf69c6c7854726800469c20ade

sha512: e3d4bf15d4cbb0a3703350ffce4024d6b3a44d56ad0e4fc12085b9ef70b741996a8c0af72aea21840e4e2e04dbad760978312995b3e426c15524facce8f181a7

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 1a30de546989c1dab21b3faa1c85baa0ebb4ef71a20a4f510998a7ae72655b31

Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
mobi.firedepartment.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
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
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.ACCESS_AD SERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_AD_SERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
mobi.firedepartment.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS	
e5f97f6dce976c0d1dbb58ecbdd8747d.apk	FINDINGS	DETAILS
	Anti-VM Code	possible VM check
classes.dex	FINDINGS	DETAILS
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check
	Compiler	unknown (please file detection issue!)

FILE	DETAILS	
classes2.dex	FINDINGS	DETAILS
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti Debug Code	Debug.isDebuggerConnected() check
	Anti-VM Code	Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check
	Compiler	unknown (please file detection issue!)
classes3.dex	FINDINGS	DETAILS
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti-VM Code	network operator name check
	Compiler	unknown (please file detection issue!)

ACTIVITY	INTENT
mobi.firedepartment.ui.views.incidents.HomeActivity	Schemes: https://, Hosts: www.pulsepoint.org, Path Patterns: /appdeeplink/home,
mobi.firedepartment.ui.views.agencies.AgencySearchActivity	Schemes: https://, Hosts: www.pulsepoint.org, Path Patterns: /appdeeplink/agency-search,
mobi.firedepartment.ui.views.agencies.AgencyProfileActivity	Schemes: https://, Hosts: www.pulsepoint.org, Path Patterns: /appdeeplink/agency-profile/10,
mobi.firedepartment.ui.views.notifications.NotificationsActivity	Schemes: https://, Hosts: www.pulsepoint.org, Path Patterns: /appdeeplink/notification-settings,
mobi.firedepartment.ui.views.more.CPRHowToActivity	Schemes: https://, Hosts: www.pulsepoint.org, Path Patterns: /appdeeplink/cpr-how-to,
mobi.firedepartment.ui.views.notifications.TroubleshootNotificationsActivity	Schemes: https://, Hosts: www.pulsepoint.org, Path Patterns: /appdeeplink/fix-notifications,
mobi.firedepartment.ui.views.agencies.AgencyCoverageMapActivity	Schemes: https://, Hosts: www.pulsepoint.org, Path Patterns: /appdeeplink/coverage-map,
mobi.firedepartment.ui.views.more.AEDHowToActivity	Schemes: https://, Hosts: www.pulsepoint.org, Path Patterns: /appdeeplink/aed-how-to,
mobi.firedepartment.ui.views.more.MoreActivity	Schemes: https://, Hosts: www.pulsepoint.org, Path Patterns: /appdeeplink/more,

ACTIVITY	INTENT
mobi.firedepartment.ui.views.more.UnitLegendActivity	Schemes: https://, Hosts: www.pulsepoint.org, Path Patterns: /appdeeplink/unit-status-legend,
mobi.firedepartment.ui.views.incidents.detail.IncidentDetailActivity	Schemes: https://, Hosts: web.pulsepoint.org,
mobi.firedepartment.ui.views.verifiedresponder.VerifiedRegActivity	Schemes: https://, Hosts: api.pulsepoint.org, Path Patterns: /register/.*,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	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	Broadcast Receiver (com.google.android.gms.gcm.GcmReceiver) 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.
3	Broadcast Receiver (mobi.firedepartment.receivers.PhoneStartBroadcastReceiver) 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.
4	Activity (mobi.firedepartment.ui.views.incidents.HomeActivity) 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.
5	Activity (mobi.firedepartment.ui.views.agencies.AgencySearchActivity) 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.
6	Activity (mobi.firedepartment.ui.views.agencies.AgencyProfileActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Activity (mobi.firedepartment.ui.views.notifications.NotificationsActivity) 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.
8	Activity (mobi.firedepartment.ui.views.more.CPRHowToActivity) 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.
9	Activity (mobi.firedepartment.ui.views.debug.DebugModeActivity) 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 (mobi.firedepartment.ui.views.notifications.TroubleshootNotificationsActivity) 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.
11	Activity (mobi.firedepartment.ui.views.agencies.AgencyCoverageMapActivity) 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 (mobi.firedepartment.ui.views.cprmode.VerifiedBadgeActivity) 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.
13	Activity (mobi.firedepartment.ui.views.more.AEDHowToActivity) 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	Activity (mobi.firedepartment.ui.views.more.MoreActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
15	Activity (mobi.firedepartment.ui.views.more.UnitLegendActivity) 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.
16	Activity (mobi.firedepartment.ui.views.incidents.detail.IncidentDetailActivity) 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.
17	Activity (mobi.firedepartment.ui.views.more.support.FeedbackActivity) 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	Activity (mobi.firedepartment.ui.views.more.support.SupportActivity) 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.
19	Activity (mobi.firedepartment.ui.views.more.PreferencesActivity) 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.
20	Activity (mobi.firedepartment.ui.views.more.support.SupportItemActivity) 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.
21	Activity (mobi.firedepartment.ui.views.incidents.map.StreetViewPanoActivity) 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.
22	Activity (mobi.firedepartment.ui.views.incidents.detail.IncidentStreetViewPanoActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
23	Activity (mobi.firedepartment.ui.views.incidents.detail.IncidentMapActivity) 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.
24	Activity (mobi.firedepartment.ui.views.maplayers.PrePlanActivity) 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.
25	Activity (mobi.firedepartment.ui.views.incidents.map.IncidentAEDActivity) 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.
26	Activity (mobi.firedepartment.ui.views.agencies.AgencyFeedActivity) 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.
27	Activity (mobi.firedepartment.ui.views.agencies.AgencyUnitStatusActivity) 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.
28	Activity (mobi.firedepartment.ui.views.maplayers.StationListActivity) 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.
29	Activity (mobi.firedepartment.ui.views.maplayers.MapLayerItemProfileActivity) 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.
30	Activity (mobi.firedepartment.ui.views.verifiedresponder.VRHomeActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
31	Activity (mobi.firedepartment.ui.views.verifiedresponder.VRDutySubscriptionActivity) 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.
32	Activity (mobi.firedepartment.ui.views.verifiedresponder.VRAgenciesActivity) 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.
33	Activity (mobi.firedepartment.ui.views.verifiedresponder.VRUnitGroupsActivity) 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.
34	Activity (mobi.firedepartment.ui.views.pulsepointaed.PulsePointAEDActivity) 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.
35	Activity (mobi.firedepartment.ui.views.ftu.FTUActivity) 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.
36	Activity (mobi.firedepartment.ui.views.verifiedresponder.VerifiedRegActivity) 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.
37	Activity (mobi.firedepartment.ui.views.cprmode.ActiveCPRAActivity) 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.
38	Activity (mobi.firedepartment.ui.views.more.CPRLearnMoreActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
39	Activity (mobi.firedepartment.ui.views.survey.NativeSurveyActivity) 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.
40	Activity (mobi.firedepartment.ui.views.agencies.AgencyShapeActivity) 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.
41	Activity (mobi.firedepartment.ui.views.incidents.AlertDetailActivity) 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.
42	Service (co.mobiwise.library.media.MediaPlayerService) 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.
43	Service (co.mobiwise.library.radio.RadioPlayerService) 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.
44	Broadcast Receiver (co.mobiwise.library.broadcast.PlayerControllerBroadcast) 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.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 1 | INFO: 2 | SECURE: 1 | 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	butterknife/ButterKnife.java co/mobiwise/library/media/MediaManager.java co/mobiwise/library/radio/RadioManager.java co/mobiwise/library/radio/RadioPlayerService.java com/spoledge/aacdecoder/AACPlayer.java com/spoledge/aacdecoder/BufferReader.java com/spoledge/aacdecoder/FlashAACInputStream.java com/spoledge/aacdecoder/IcyInputStream.java com/spoledge/aacdecoder/MP3Player.java com/spoledge/aacdecoder/MultiPlayer.java com/spoledge/aacdecoder/PCMFeed.java mobi/firedepartment/services/GcmIntentService.java mobi/firedepartment/services/LocationUpdateService.java mobi/firedepartment/ui/views/verifiedresponder/VRHomeActivity.java org/codechimp/apprater/AppRater.java retrofit/Platform.java retrofit/android/AndroidLog.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	com/spoledge/aacdecoder/AACPlayer.java com/spoledge/aacdecoder/FlashAACInputStream.java mobi/firedepartment/PulsepointApp.java mobi/firedepartment/services/RestClient.java mobi/firedepartment/ui/views/debug/DebugMainFragment.java mobi/firedepartment/ui/views/incidents/detail/IncidentMapActivity.java mobi/firedepartment/ui/views/incidents/detail/IncidentStreetViewPanoActivity.java mobi/firedepartment/ui/views/incidents/map/IncidentAEDActivity.java mobi/firedepartment/ui/views/incidents/map/IncidentMapFragment.java mobi/firedepartment/ui/views/incidents/map/StreetViewPanoActivity.java mobi/firedepartment/ui/views/maplayers/MapLayerItemProfileActivity.java mobi/firedepartment/ui/views/maplayers/PrePlanActivity.java mobi/firedepartment/ui/views/survey/SurveyQuestionFragment.java mobi/firedepartment/ui/views/verifiedresponder/VRAgenciesActivity.java mobi/firedepartment/ui/views/verifiedresponder/VRDutySubscriptionActivity.java mobi/firedepartment/ui/views/verifiedresponder/VRUnitGroupsActivity.java mobi/firedepartment/utils/AppKeys.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	mobi/firedepartment/services/RestClient.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/spoledge/aacdecoder/BuildConfig.java
5	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	mobi/firedepartment/ui/views/incidents/detail/IncidentDetailActivity.java

SHARED LIBRARY BINARY ANALYSIS

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libaacdecoder.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	x86_64/libaacdecoder.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	armeabi-v7a/libaacdecoder.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86/libaacdecoder.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libaacdecoder.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	x86_64/libaacdecoder.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	armeabi-v7a/libaacdecoder.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86/libaacdecoder.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.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	mobi/firedepartment/PulsepointApp.java mobi/firedepartment/ui/utis/PulsePointDialogs.java org/codechimp/apprater/AmazonMarket.java org/codechimp/apprater/GoogleMarket.java
00125	Check if the given file path exist	file	mobi/firedepartment/ui/views/maplayers/PrePlanActivity.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	mobi/firedepartment/services/GcmIntentService.java mobi/firedepartment/ui/utis/PulsePointDialogs.java mobi/firedepartment/ui/views/agencies/AgencyProfileActivity.java mobi/firedepartment/ui/views/agencies/AgencyUnitStatusActivity.java mobi/firedepartment/ui/views/cprmode/ActiveCPRActivity.java mobi/firedepartment/ui/views/debug/DebugMainFragement.java mobi/firedepartment/ui/views/incidents/detail/IncidentDetailActivity.java mobi/firedepartment/ui/views/incidents/detail/IncidentMapActivity.java mobi/firedepartment/ui/views/incidents/detail/IncidentStreetViewPanoActivity.java mobi/firedepartment/ui/views/splashscreen/SplashScreenActivity.java mobi/firedepartment/ui/views/verifiedresponder/VRHomeActivity.java
00013	Read file and put it into a stream	file	com/spoledge/aacdecoder/AACPlayer.java com/spoledge/aacdecoder/FlashAACPlayer.java okio/Okio.java retrofit/mime/TypedFile.java
00091	Retrieve data from broadcast	collection	mobi/firedepartment/ui/views/agencies/AgencyProfileActivity.java mobi/firedepartment/ui/views/agencies/AgencyUnitStatusActivity.java mobi/firedepartment/ui/views/maplayers/MapLayerItemProfileActivity.java mobi/firedepartment/ui/views/maplayers/StationListActivity.java mobi/firedepartment/ui/views/verifiedresponder/VRDutySubscriptionActivity.java
00096	Connect to a URL and set request method	command network	retrofit/client/URLConnectionClient.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/spoledge/aacdecoder/AACPlayer.java retrofit/client/URLConnectionClient.java
00109	Connect to a URL and get the response code	network command	com/spoledge/aacdecoder/AACPlayer.java retrofit/client/URLConnectionClient.java
00056	Modify voice volume	control	mobi/firedepartment/ui/views/notifications/TroubleshootNotificationsActivity.java
00016	Get location info of the device and put it to JSON object	location collection	mobi/firedepartment/ui/views/agencies/AgencyCoverageMapActivity.java
00030	Connect to the remote server through the given URL	network	com/spoledge/aacdecoder/AACPlayer.java
00023	Start another application from current application	reflection control	mobi/firedepartment/PulsepointApp.java
00022	Open a file from given absolute path of the file	file	com/jakewharton/picasso/OkHttp3Downloader.java retrofit/mime/TypedFile.java
00033	Query the IMEI number	collection	mobi/firedepartment/utis/DeviceID.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	mobi/firedepartment/ui/utis/PulsePointDialogs.java mobi/firedepartment/ui/views/debug/DebugMainFragment.java mobi/firedepartment/ui/views/splashscreen/SplashScreenActivity.java
00162	Create InetAddress object and connecting to it	socket	com/spoledge/aacdecoder/IcyURLConnection.java
00163	Create new Socket and connecting to it	socket	com/spoledge/aacdecoder/IcyURLConnection.java
00108	Read the input stream from given URL	network command	com/spoledge/aacdecoder/IcyURLConnection.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://respond-e6ebe.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebase-remoteconfig.googleapis.com/v1/projects/692743675601/namespaces/firebase:fetch?key=AlzaSyDXrnlFEGTkvRaTb7AIYk02NphggIAow7c . This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.READ_PHONE_STATE
Other Common Permissions	6/44	android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.ACCESS_NOTIFICATION_POLICY, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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
respond-e6ebe.firebaseio.com	ok	IP: 35.190.39.113 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
web.pulsepoint.org	ok	IP: 18.155.173.27 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
184.82.135.71	ok	IP: 184.82.135.71 Country: Thailand Region: Krung Thep Maha Nakhon City: Bangkok Latitude: 13.750000 Longitude: 100.516670 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.flickr.com	ok	IP: 18.155.176.124 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
www.amazon.com	ok	IP: 18.238.90.46 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
www.facebook.com	ok	IP: 31.13.70.36 Country: United States of America Region: California City: Los Angeles Latitude: 34.052231 Longitude: -118.243683 View: Google Map
www.linkedin.com	ok	IP: 172.64.146.215 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.youtube.com	ok	IP: 142.250.74.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.twitter.com	ok	IP: 162.159.140.229 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
www.instagram.com	ok	IP: 157.240.11.174 Country: United States of America Region: California City: Los Angeles Latitude: 34.052231 Longitude: -118.243683 View: Google Map

EMAILS

EMAIL	FILE
feedback@pulsepoint.org	mobi/firedepartment/ui/views/debug/DebugMainFragment.java

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"AED.Password" : "Password"
"AED.CurrentPassword" : "□□□□□□□□"
"Respond.Notification.Troubleshoot.BadGCMTOKEN" : "□□□GCM□□□□□□□□□□□□□□□□□□"
"AED.Password" : "□□□□□"
"AED.ResetPassword" : "□□□□□□□□□□□□"
"AED.Password" : "Contraseña"
"AED.InvalidEmailOrPassword" : "□□□□□□□□□□□□□□□□□□"
"firebase_database_url" : "https://respond-e6ebe.firebaseio.com"
"Respond.Notification.Troubleshoot.Check.Token" : "□□□□□□"

POSSIBLE SECRETS
"AED.CommunityUser" : "□□□□□□□□□□"
"google_crash_reporting_api_key" : "AlzaSyDXrniFEGTkVraTb7AlYk02NphggIAow7c"
"Test.Key" : "□□□□□□□□□□□□□□YAY"
"Respond.Notification.Troubleshoot.NoGCMToken" : "□□□GCM□□□□□□□□□□"
"google_api_key" : "AlzaSyDXrniFEGTkVraTb7AlYk02NphggIAow7c"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
23456789abcdefghijklmnopqrstuvwxyz
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
258EAFa5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
9a04f079-9840-4286-ab92-e65be0885f95
e2719d58-a985-b3c9-781a-b030af78d30e

PLAYSTORE INFORMATION

Title: PulsePoint Respond

Score: 4.6331863 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** Category: Medical **Play Store URL:** [mobi.firedepartment](https://play.google.com/store/apps/details?id=com.pulsepoint.respond)

Developer Details: PulsePoint Foundation, PulsePoint+Foundation, None, <https://www.pulsepoint.org>, support@pulsepoint.org,

Release Date: Dec 22, 2011 **Privacy Policy:** [Privacy link](#)

Description:

PulsePoint Respond is a 911-connected app that can immediately inform you of emergencies occurring in your community and can request your help when CPR is needed nearby. PulsePoint helps create an informed and engaged community that drives a “Culture of Action,” a key strategy in strengthening the Chain of Survival for cardiac arrest victims. In addition to nearby “CPR-needed” notifications, you can choose to be notified of significant events that may impact you and your family. These informational notifications provide an early heads-up to local threats such as wildland fires, flooding and utility emergencies. You can even monitor live dispatch radio traffic for most PulsePoint-connected communities with a simple tap on the speaker icon. PulsePoint currently provides coverage for thousands of cities and communities, with many more on the way. For more information, visit pulsepoint.org, contact us at info@pulsepoint.org, or join the conversation at Facebook and Twitter. PulsePoint not yet available in your community? Although we are working hard to make public safety agencies aware of PulsePoint, you can help by expressing interest to your local fire chief, EMS official, and elected officials such as your mayor, council member or supervisor. A simple note, phone call or public meeting comment would ensure that they are aware of PulsePoint. We have found that City Hall does listen and is quite willing to bring PulsePoint to the community. PulsePoint is a 501(c)(3) public non-profit foundation.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 14:34:34	Generating Hashes	OK
2025-09-01 14:34:34	Extracting APK	OK
2025-09-01 14:34:34	Unzipping	OK
2025-09-01 14:34:34	Parsing APK with androguard	OK
2025-09-01 14:34:34	Extracting APK features using aapt/aapt2	OK
2025-09-01 14:34:35	Getting Hardcoded Certificates/Keystores	OK

2025-09-01 14:34:37	Parsing AndroidManifest.xml	OK
2025-09-01 14:34:37	Extracting Manifest Data	OK
2025-09-01 14:34:37	Manifest Analysis Started	OK
2025-09-01 14:34:40	Performing Static Analysis on: PulsePoint (mobi.firedepartment)	OK
2025-09-01 14:34:41	Fetching Details from Play Store: mobi.firedepartment	OK
2025-09-01 14:34:43	Checking for Malware Permissions	OK
2025-09-01 14:34:43	Fetching icon path	OK
2025-09-01 14:34:43	Library Binary Analysis Started	OK
2025-09-01 14:34:43	Analyzing lib/arm64-v8a/libaacdecoder.so	OK
2025-09-01 14:34:43	Analyzing lib/x86_64/libaacdecoder.so	OK
2025-09-01 14:34:43	Analyzing lib/armeabi-v7a/libaacdecoder.so	OK

2025-09-01 14:34:43	Analyzing lib/x86/libaacdecoder.so	OK
2025-09-01 14:34:43	Analyzing apktool_out/lib/arm64-v8a/libaacdecoder.so	OK
2025-09-01 14:34:43	Analyzing apktool_out/lib/x86_64/libaacdecoder.so	OK
2025-09-01 14:34:43	Analyzing apktool_out/lib/armeabi-v7a/libaacdecoder.so	OK
2025-09-01 14:34:43	Analyzing apktool_out/lib/x86/libaacdecoder.so	OK
2025-09-01 14:34:43	Reading Code Signing Certificate	OK
2025-09-01 14:34:43	Running APKiD 2.1.5	OK
2025-09-01 14:34:46	Detecting Trackers	OK
2025-09-01 14:34:49	Decompiling APK to Java with JADX	OK
2025-09-01 14:35:22	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 14:35:22	Decompiling classes2.dex with JADX	OK

2025-09-01 14:35:31	Decompiling classes.dex with JADX	OK
2025-09-01 14:35:40	Decompiling classes3.dex with JADX	OK
2025-09-01 14:35:43	Decompiling classes2.dex with JADX	OK
2025-09-01 14:35:52	Decompiling classes.dex with JADX	OK
2025-09-01 14:36:00	Decompiling classes3.dex with JADX	OK
2025-09-01 14:36:04	Converting DEX to Smali	OK
2025-09-01 14:36:04	Code Analysis Started on - java_source	OK
2025-09-01 14:36:05	Android SBOM Analysis Completed	OK
2025-09-01 14:36:09	Android SAST Completed	OK
2025-09-01 14:36:10	Android API Analysis Started	OK
2025-09-01 14:36:12	Android API Analysis Completed	OK

2025-09-01 14:36:13	Android Permission Mapping Started	OK
2025-09-01 14:36:15	Android Permission Mapping Completed	OK
2025-09-01 14:36:16	Android Behaviour Analysis Started	OK
2025-09-01 14:36:19	Android Behaviour Analysis Completed	OK
2025-09-01 14:36:19	Extracting Emails and URLs from Source Code	OK
2025-09-01 14:36:19	Email and URL Extraction Completed	OK
2025-09-01 14:36:19	Extracting String data from APK	OK
2025-09-01 14:36:20	Extracting String data from SO	OK
2025-09-01 14:36:20	Extracting String data from Code	OK
2025-09-01 14:36:20	Extracting String values and entropies from Code	OK
2025-09-01 14:36:23	Performing Malware check on extracted domains	OK

2025-09-01 14:36:27	Saving to Database	OK
---------------------	--------------------	----

Report Generated by - MobSF v4.4.0

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.

© 2025 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).