MOBSF

ANDROID STATIC ANALYSIS REPORT

Play services (3.11.3)

File Name:	umobix__3523039__.apk
Package Name:	com.play.services
Scan Date:	Aug. 10, 2024, 7:35 p.m.

App Security Score: 44/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
7	30	1	2	1

FILE INFORMATION

File Name: umobix___3523039___.apk
Size: 11.6MB

MD5: 7eb8ee546cf6e07d3a887cca56bd0fe4
SHA1: 0fcace8bf5b051c8775b99792b22745500eaa581
SHA256: 6f4b110d1e030b26d25070cb96b25839227dd4bbada89103ac812c626daaaf8d

APP INFORMATION

App Name: Play services
Package Name: com.play.services
Main Activity: c.a.b.app.ui.activity.LoadActivity
Target SDK: 28
Min SDK: 22
Max SDK:
Android Version Name: 3.11.3
Android Version Code: 179

APP COMPONENTS

Activities: 33
Services: 28
Receivers: 9
Providers: 6
Exported Activities: 6
Exported Services: 7
Exported Receivers: 6
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=CODE, ST=STATE, L=CITY, O=ORGANIZATION, OU=UNIT, CN=NAME
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-11-18 13:38:37+00:00
Valid To: 2046-11-12 13:38:37+00:00
Issuer: C=CODE, ST=STATE, L=CITY, O=ORGANIZATION, OU=UNIT, CN=NAME
Serial Number: 0x5e26cd7b
Hash Algorithm: sha256
md5: 884ebb2ea7b7e7b713fdb8b5a7f28885
sha1: f4e6da34f0071aeb70010ebb69875e5212d69140
sha256: 80577c5864eee7e8b8f6883d8fd292de441c5316612da4f6d6f1738848d8be64
sha512: 8d45481304a833d8cce59a3159c86fe5c66985725afd75a298d07f723fc2c2a51f7b07a4c8714602ceb70a5e66de20d69858195d06bfae8536c415f4184cde78
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: cf1a21c6ddf1b17176a3685f355633ae881e5e3672da19743165b2a0c5f419b2
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
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.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.CHANGE_CONFIGURATION	SignatureOrSystem	change your UI settings	Allows an application to change the current configuration, such as the locale or overall font size.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.RECEIVE_WAP_PUSH	dangerous	receive WAP	Allows application to receive and process WAP messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.READ_SYNC_SETTINGS	normal	read sync settings	Allows an application to read the sync settings, such as whether sync is enabled for Contacts.
android.permission.WRITE_SYNC_SETTINGS	normal	write sync settings	Allows an application to modify the sync settings, such as whether sync is enabled for Contacts.
android.permission.READ_SYNC_STATS	normal	read sync statistics	Allows an application to read the sync stats; e.g. the history of syncs that have occurred.
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.WRITE_CALL_LOG	dangerous	allows writing to (but not reading) the user's call log.	Allows an application to write (but not read) the user's call log data.
android.permission.READ_CALL_LOG	dangerous	grants read access to the user's call log.	Allows an application to read the user's call log.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.ANSWER_PHONE_CALLS	dangerous	permits an app to answer incoming phone calls.	Allows the app to answer an incoming phone call.
android.permission.PROCESS_OUTGOING_CALLS	dangerous	intercept outgoing calls	Allows application to process outgoing calls and change the number to be dialled. Malicious applications may monitor, redirect or prevent outgoing calls.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.WRITE_SMS	dangerous	edit SMS or MMS	Allows application to write to SMS messages stored on your phone or SIM card. Malicious applications may delete your messages.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.RECEIVE_MMS	dangerous	receive MMS	Allows application to receive and process MMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
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_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.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.browser.permission.READ_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.SYSTEM_OVERLAY_WINDOW	unknown	Unknown permission	Unknown permission from android reference
android.permission.INTERNAL_SYSTEM_WINDOW	signature	display unauthorised windows	Allows the creation of windows that are intended to be used by the internal system user interface. Not for use by common applications.
android.permission.READ_PRIVILEGED_PHONE_STATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
android.permission.ACCESS_RESTRICTED_SETTINGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	normal	enables foreground services for media playback.	Allows a regular application to use Service.startForeground with the type "mediaPlayback".
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>/home/mobsf/.MobSF/uploads/7eb8ee546cf6e07d3a887cca56bd0fe4/7eb8ee546cf6e07d3a887cca56bd0fe4.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Protector</td><td>FreeRASP</td></tr>
</table>
</td></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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator check
network operator name check
device ID check
subscriber ID check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
c.a.b.lock.ui.activity.ComposeSmsActivity	Schemes: sms://, smsto://, mms://, mmsto://,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

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: 7 | WARNING: 19 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.1-5.1.1, [minSdk=22]	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	App is direct-boot aware [android:directBootAware=true]	info	This app can run before the user unlocks the device. If you're using a custom subclass of Application, and if any component inside your application is direct - boot aware, then your entire custom application is considered to be direct - boot aware.During Direct Boot, your application can only access the data that is stored in device protected storage.
4	Activity (com.play.services.PLACEHOLDER) 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.
5	Activity-Alias (com.play.services.PLACEHOLDER) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Activity (com.play.services.PRODUCT) 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.
7	Activity-Alias (com.play.services.PRODUCT) 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.
8	Activity (c.a.b.core.ui.activity.KeepAliveServiceStartActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (28) of the app to 29 or higher to fix this issue at platform level.
9	Activity (c.a.b.core.ui.activity.KeepAliveServiceStartActivity) 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	Broadcast Receiver (c.a.b.app.receiver.MainReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
11	Broadcast Receiver (c.a.b.app.receiver.ForceReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
12	Broadcast Receiver (c.a.b.app.receiver.AdminReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_DEVICE_ADMIN [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.
13	Service (c.a.b.core.service.AccessibilityService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [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. 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.
14	Service (c.a.b.core.service.KeepAliveJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [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. 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
15	Service (c.a.b.core.service.KeepAliveLocalService) 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.
16	Service (c.a.b.core.service.KeepAliveRemoteService) 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.
17	Service (c.a.b.auth.service.AuthenticationService) 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.
18	Service (c.a.b.auth.service.SyncAccountService) 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.
19	Broadcast Receiver (c.a.b.lock.receiver.SmsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BROADCAST_SMS [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
20	Broadcast Receiver (c.a.b.lock.receiver.MmsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BROADCAST_WAP_PUSH [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.
21	Activity (c.a.b.lock.ui.activity.ComposeSmsActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
22	Service (c.a.b.lock.service.HeadlessSmsSendService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.SEND_RESPOND_VIA_MESSAGE [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. 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.
23	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
24	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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.
25	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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 (com.google.firebase.auth.internal.RecaptchaActivity) 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.
27	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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.

</> CODE ANALYSIS

HIGH: **0** | WARNING: **8** | INFO: **1** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	ad/b.java an/e0.java b2/n.java bh/h.java bh/i.java bh/k7.java bh/w7.java bh/x2.java cc/b.java ch/qos/logback/classic/android/SQLiteAppender.java d3/c.java ec/a.java ec/b.java f2/a.java f8/c.java f8/d.java j5/a.java j8/a.java ja/d.java k9/a.java kd/c.java l8/a.java p002if/n.java p002if/t.java p5/c.java pe/a.java pe/d.java q/c.java ra/a.java rb/b.java re/a.java s7/a.java s7/f.java tc/a.java ue/p.java v7/b.java vb/a.java vd/b.java vd/c.java wj/q0.java wj/s0.java wj/w0.java xd/a.java yd/a.java z9/b.java z9/c.java z9/e.java zd/a.java
				ah/a.java ai/a.java aj/c0.java aj/d0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				aj/e.java aj/f.java aj/g0.java aj/h0.java aj/k0.java aj/m.java aj/m0.java aj/n.java aj/o.java aj/q.java aj/r.java aj/u.java aj/v.java aj/w.java aj/w0.java aj/y.java al/c.java b2/c0.java b2/d0.java b2/e0.java b2/o.java bf/b.java bh/d3.java bh/g4.java bh/k7.java bh/x7.java bj/b.java bj/d.java bl/h.java bn/c.java c/a/b/Application.java c/a/b/core/utils/other/f.java ch/qos/logback/classic/android/LogcatAppender.java ch/qos/logback/classic/net/SimpleSocketServer.java ch/qos/logback/classic/pattern/TargetLengthBasedClassNameAbbreviator.java ch/qos/logback/classic/spi/ThrowableProxy.java ch/qos/logback/core/joran/util/ConfigurationWatchListUtil.java ch/qos/logback/core/net/DefaultSocketConnector.java ch/qos/logback/core/net/SocketConnectorBase.java ch/qos/logback/core/subst/Node.java cl/l.java cl/p.java d1/d.java d1/e.java d1/j.java d2/b.java df/i.java dg/a.java dh/a.java dl/a.java dl/b.java dl/f.java e2/c.java ef/k.java eg/e.java eg/o.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				eg/p.java ej/a.java el/a.java f2/b.java fh/a.java fj/e.java fj/f.java fk/d.java g0/a.java g1/g.java g1/i.java gh/a.java gh/b.java h1/a.java h1/e.java h2/c.java h2/g.java hf/d.java hj/a.java hj/c.java hj/d.java hk/b.java ik/c.java in/h.java j0/f.java jg/b.java jh/g.java jj/a.java jn/d.java kd/a.java ki/a.java ki/c.java kk/a.java kk/b0.java kk/c.java kk/c0.java kk/d0.java kk/e0.java kk/f.java kk/h0.java kk/i0.java kk/j.java kk/l.java kk/m.java kk/m0.java kk/o0.java kk/t.java kk/v.java kk/w.java kk/x.java kk/y.java l/l.java lj/a.java m1/f.java m9/b.java m9/c.java mk/b.java
2	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	

NO	ISSUE	SEVERITY	STANDARDS	FILES
				n/f.java net/majorkernelpanic/streaming/gl/SurfaceView.java org/slf4j/helpers/Util.java p002if/n.java p1/b.java q/c.java qg/r.java qk/a.java qk/b.java r1/b.java rf/a.java rf/e.java rf/f.java rf/i.java rf/k.java rf/n.java rf/o.java rf/p.java rf/r.java rf/t.java rg/o.java rl/a.java rm/a.java rm/f.java s1/c.java sf/c.java sf/d.java sf/f.java sf/g.java sf/j.java sf/r.java sf/v.java sm/b.java sm/e.java t0/d.java tm/c.java u0/m.java u0/p.java u2/b.java ue/f.java ue/n.java ue/p.java ue/r.java uf/c0.java uf/f.java uf/g0.java uf/g2.java uf/i0.java uf/k0.java uf/m1.java uf/n0.java uf/w0.java uf/y0.java ui/k.java ui/n.java um/a.java um/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				vi/i.java vl/i.java vm/b.java wh/d.java wi/c.java wi/e.java wi/g.java x0/b.java x0/c.java x0/d.java xh/b.java xi/b.java xm/a.java xm/b.java xm/c.java xm/e.java xm/f.java xm/g.java xm/h.java y0/e.java y0/f.java y0/g.java y0/h.java y0/j.java y0/k.java y0/l.java y0/n.java y1/a.java yf/a.java yi/c.java yi/d.java ym/a.java z0/a.java z0/b.java z0/f.java z1/a.java z1/b.java z1/d.java zh/g.java zi/c.java zm/b.java zm/c.java zm/d.java zm/e.java zm/f.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	c/a/b/core/utils/other/b.java c/b.java ch/qos/logback/core/android/AndroidContextUtil.java ja/d.java o5/h.java oe/g.java sm/b.java yb/c.java zm/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	ao/a.java bo/a.java co/a.java eo/a.java fo/a.java ho/a.java io/c.java io/i.java jo/a.java oo/c.java p001do/a.java rm/c.java xn/a.java yn/a.java zn/a.java
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	c/a/b/Application.java ch/qos/logback/core/net/ssl/SSLContextFactoryBean.java in/c.java in/d.java in/g.java in/h.java q3/a.java z8/e.java
6	MD5 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	bh/q7.java ym/a.java
7	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	al/h.java bh/q7.java dl/c.java g/b.java j/c.java q/e.java rm/a.java sl/e0.java sl/g0.java sl/t2.java te/a.java tl/h.java wk/c.java xm/d.java yl/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	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	ak/f0.java ch/qos/logback/classic/joran/action/ConfigurationAction.java ch/qos/logback/classic/sift/ContextBasedDiscriminator.java ch/qos/logback/core/CoreConstants.java ch/qos/logback/core/net/ssl/SSL.java ch/qos/logback/core/rolling/helper/DateTokenConverter.java ch/qos/logback/core/rolling/helper/IntegerTokenConverter.java g4/n.java i9/h.java tl/g.java xj/i.java yj/e.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	aj/e.java bh/g4.java
10	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	aj/e.java eg/a.java hk/b.java kk/t.java sf/v.java
11	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	hk/c.java wb/a.java z1/d.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libpbkdf2_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/libclib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
3	armeabi-v7a/libsecurity.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__vsprintf_chk', '__strlen_chk']	False warning Symbols are available.
4	armeabi-v7a/libpolarssl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__memcpy_chk']	False warning Symbols are available.
5	x86_64/libpbkdf2_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	x86_64/libclib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__FD_SET_chk']	False warning Symbols are available.
7	x86_64/libsecurity.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__vsprintf_chk', '__strlen_chk']	False warning Symbols are available.
8	x86_64/libpolarssl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__memcpy_chk']	False warning Symbols are available.
9	arm64-v8a/libpbkdf2_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	arm64-v8a/libclib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__FD_SET_chk']	False warning Symbols are available.
11	arm64-v8a/libsecurity.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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', '__vsprintf_chk']	False warning Symbols are available.
12	arm64-v8a/libpolarssl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__memcpy_chk']	False warning Symbols are available.
13	x86/libpbkdf2_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	x86/libclib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
15	x86/libsecurity.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__vsprintf_chk', '__strlen_chk']	False warning Symbols are available.
16	x86/libpolarssl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__memcpy_chk']	False warning Symbols are available.
17	armeabi-v7a/libpbkdf2_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	armeabi-v7a/libclib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
19	armeabi-v7a/libsecurity.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__vsprintf_chk', '__strlen_chk']	False warning Symbols are available.
20	armeabi-v7a/libpolarssl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__memcpy_chk']	False warning Symbols are available.
21	x86_64/libpbkdf2_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	x86_64/libclib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__FD_SET_chk']	False warning Symbols are available.
23	x86_64/libsecurity.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__vsprintf_chk', '__strlen_chk']	False warning Symbols are available.
24	x86_64/libpolarssl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__memcpy_chk']	False warning Symbols are available.
25	arm64-v8a/libpbkdf2_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	arm64-v8a/libclib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__FD_SET_chk']	False warning Symbols are available.
27	arm64-v8a/libsecurity.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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', '__vsprintf_chk']	False warning Symbols are available.
28	arm64-v8a/libpolarssl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__memcpy_chk']	False warning Symbols are available.
29	x86/libpbkdf2_native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
30	x86/libclib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
31	x86/libsecurity.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__vsprintf_chk', '__strlen_chk']	False warning Symbols are available.
32	x86/libpolarssl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__memcpy_chk']	False warning Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	20/24	android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.WRITE_SETTINGS, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.READ_PHONE_STATE, android.permission.READ_CALL_LOG, android.permission.GET_ACCOUNTS, android.permission.SEND_SMS, android.permission.READ_SMS, android.permission.RECEIVE_SMS, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.READ_CONTACTS, android.permission.SYSTEM_ALERT_WINDOW
Other Common Permissions	15/45	android.permission.AUTHENTICATE_ACCOUNTS, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.REQUEST_INSTALL_PACKAGES, android.permission.CHANGE_NETWORK_STATE, android.permission.CHANGE_WIFI_STATE, android.permission.CALL_PHONE, android.permission.PROCESS_OUTGOING_CALLS, android.permission.ACCESS_NOTIFICATION_POLICY, android.permission.WRITE_SMS, android.permission.WRITE_CONTACTS, android.permission.READ_CALENDAR, android.permission.PACKAGE_USAGE_STATS, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, 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
www.slf4j.org	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api2.amplitude.com	ok	**IP:** 54.149.157.100 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
goo.gl	ok	**IP:** 172.217.19.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
regionconfig.eu.amplitude.com	ok	**IP:** 3.165.206.33 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.google.com	ok	**IP:** 142.250.201.196 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.180.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
logback.qos.ch	ok	**IP:** 195.15.222.169 **Country:** Switzerland **Region:** Basel-Stadt **City:** Basel **Latitude:** 47.558399 **Longitude:** 7.573270 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
google.com	ok	**IP:** 142.250.180.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
app-measurement.com	ok	**IP:** 142.251.208.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.openssl.org	ok	**IP:** 34.49.79.89 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
build-cb7af.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
update.crashlytics.com	ok	**IP:** 142.250.180.227 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
regionconfig.amplitude.com	ok	**IP:** 3.165.206.78 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.googleadservices.com	ok	**IP:** 142.251.208.98 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
console.firebase.google.com	ok	**IP:** 142.250.180.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
xml.org	ok	**IP:** 104.239.240.11 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
reports.crashlytics.com	ok	No Geolocation information available.
i.instagram.com	ok	**IP:** 31.13.84.52 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
api.eu.amplitude.com	ok	**IP:** 3.64.45.30 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebasestorage.googleapis.com	ok	**IP:** 172.217.20.10 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://build-cb7af.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
u0013android@android.com u0013android@android.com0	sf/q.java
rudolfcopenhagen@gmail.com	b1/a.java
ftp@example.com	lib/armeabi-v7a/libclib.so
ftp@example.com	lib/x86_64/libclib.so
ftp@example.com	lib/arm64-v8a/libclib.so
ftp@example.com	lib/x86/libclib.so
ftp@example.com	apktool_out/lib/armeabi-v7a/libclib.so
ftp@example.com	apktool_out/lib/x86_64/libclib.so
ftp@example.com	apktool_out/lib/arm64-v8a/libclib.so
ftp@example.com	apktool_out/lib/x86/libclib.so

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Analytics, Profiling	https://reports.exodus-privacy.eu.org/trackers/125
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
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
"firebase_database_url" : "https://build-cb7af.firebaseio.com"
"google_crash_reporting_api_key" : "AIzaSyANDBd52iHGsfN0G_vzuMK6gcVI9INQFwI"
"google_api_key" : "AIzaSyANDBd52iHGsfN0G_vzuMK6gcVI9INQFwI"
115792089210356248762697446949407573530086143415290314195533631308867097853951
50243DC75826CDC2A814363CBCF3667D6B40
50243DC7582DC1C3AD03271EABC1677C685662A3BBE218ED
512536C05A06CBE9A00C3703B6EE6A4D6657
502336D05610D898B307201EACF56D777C
5A3F19C0512DC2D7A30E3615
5A223BCB411AC9D5B5323212B2E6697741527DB6
5023358A5B0DD4D7AC0D315FB1E8796660417FBCBD
412376CC521AC8C1A01036
5023358A5807D9C5A90B3815ACF37A7321417FBEA4EA18F87D2776B4F69AD49A5D3F3D

POSSIBLE SECRETS
63071BF70238CDD2A50B3D16
1C3F21D7470DC199A012235E8AF27E777D4663B6BBA517E971
02796D9101599B83F1566A
462237C25501CFDFA00E0005B6F56B
412376C65C07D898A9032115AEE67C77
EVJN/TCMZ7GKFXUn5FVqaiFpBuPpOlLDGP3ulSHNpCXshXEpSNdbFKdWwHVuoFup
5023358A5205DCDEAE103202F7EF67766A5E69A1A6E402F87E2476FFFF
1C3C2ACB5047DFD3AD047C02ADE67A677C
502336D05610D898B103301AB8E06B5F6E5D71B4ACF9
523E3DE25C04C8D3B3110403B0F36F706356
5B2D2BF04109CFD3B3323A15
462237C25501CFDFA00E1A1FAAF36F7E635264BAA6E525F66F3067FF
1C3F21D7470DC199B2003A1F
xjQBErXUAHP5Fiy2OGaxIsJ1LRZnlXmD7KauDO7W9CY=
432D2BD75007C8D39E013B10B7E06B76
412376C64601C0D2EF11361DB0E97B6A
50243DC7582DC1C3AD03271EABC36B64665075
402833F45F09D8D0AE103E
1C3F21D7470DC199A710321CBCF06160641C48A3A6F813FD58306DFEFD969995523E
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
q1Q68gbSr2EunBKhtefssV0iPVsSUgI/oVqPT5EkVWWLAqn7uUnl8M9IRrc193ok
52283AFB5606CDD4AD0737

POSSIBLE SECRETS
132D34C35C1AC5C2A90F7318AAA7607D7B1363A6B9FB19EB6E2760BAFC9CC5DF573935C94A48C7D3B8423C1FF9E67E7B2F0228
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
5A2231D01D1BDAD5EF043A1DBCEA617C
54292CD44107DC96B30D7D15BCE57B75685272BFAC
5D2336C17606DED9AD0E3615
54292CFC4307DFD3A5343603AAEE617C
763E2ACB4148C3D5A2172103BCE32E65675A7CB6E9F913F475346DF4FDD3D39E472D78C24107C196AA072A02ADE87C77
50243DC75838DED9B1072105A0D0667B6C5B59A086E51AE0552C41F7EF9FD68B5C3E
K3ciHTzfFv48jNbIfVE5dqZAjsSALR7qTLK2cRbwd3U=
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
5B2337CF560C8CC3B20B3D16F9DF7E7D7C5674
50243DC7582DC1C3AD03271EABCA6F7C7A5571B0BDFE04FC68
523E3DE24101C8D78D0B3103B8F567777C7775A7ACE802FC7E
5023358A5701C1D9AF143A15BCE8207E7A507BAAB9EA02FA722776
502336D05610D898A20D3D05BCE97A406A407FBFBFEE04
522F3BC1401BC5D4A80E3A05A0C67E627C
50243DC7583BC5DB92072118B8EB
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
5023358A5205DCDEAE103202F7EF67766A5E69A1A6E402
57292ECD500DFFC2A01636
76222ECD4107C2DBA40C275FBEE27A40605C6497A0F913FA6E2D76E3B2DA
5023358A5507DEDBB80A3E5FB1EE6A777D5C7FA799F913F4733769

POSSIBLE SECRETS
1C3F21D7470DC199A30B3D5EAEEF677167
1C3F21D7470DC199A30B3D5EBFE6677E7C5276B6E6
72223CD65C01C8FDA41B0005B6F56B
72223CD65C01C89692261851BBF2677E7B1376BCBBAB0EA12C
721C13FB6021EBF8803606239C
QodYd1iiGym9GiGvy+5SEw8mM3D9A1zPjofiy0dxhPA=
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
XklO7OzRB/nYKluxJ5R6ZFUOTX1+QVdOIRyIlXZpNpTgXEtgHbFLDrp9Sw2pzLEm
910bc4be2ffc96db901f02ebe2e7f46d
433E31D25A04C9D1A4061212BAE27D61
57253CE55D0CDED9A8061A159AEF6F7C6856
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
UuLLTElpb3GapgO36wP979eOjuRqhTDS48Q5ODmGyn0=
412376CC521AC8C1A010365FB8F26A7B601D60A1A0E617EB63
mTNK/hSVnW4n4RLzIp0zVO6EryuXJLOUcQEmjtjB9DUY112LUWWesswdZtMa7y6p
50243DC75824C5D8A4531D04B4E56B60
5A222BD05204C0D7B50B3C1F8AE87B606C56
w2Yi1Oh/+ojvmOXI2J8V49D6I1wst7r+nL6ZGj9lxx4=
470fa2b4ae81cd56ecbcda9735803434cec591fa
5023358A4107C3C2B10E2602F7EC677C68
763E2ACB4148DBDEA80E3651B5E86F76665D77F388C025
5A3F0BDD401CC9DB91103C01BCF57A6B4A4265B2A5DF19

POSSIBLE SECRETS
5A3F00D45C1BC9D297072102B0E86053795279BFA8E91AFC
5B2337CF560C8CC3B20B3D16F9D47B707C4762B2BDEE
gVM0JRg+DOkrsI9oCHxtH1dgXrNfriVsgZHgDDAoqJrGM375bLO+YYbLV1Zmqbos
11283DD25A0BC9FFA540690AD3A72E322F1330F1A8E512EB752B60D3FED18DDD
dW/qTgfnk+N3jTeFG+isrkHYAmK5rvVNrAs0jV9mlQw+GJB5Wra2UekuWLdZk5+S
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
75232DCA5748F4C6AE113615F9F16B607C5A7FBDE9
50243DC7583BD8D7A2090703B8E46B
523E3DF0561BD8FDA41B2034B7E66C7E6A57
43292AD75A1BD898AC033418AAEC207A665775
523E3DE54303DFF7B7033A1DB8E56277
o3sCvRiU+Z55Vq2c5MFpXXz5zhAwK6As2YFncq0GyBE=
5023358A5B1DCDC1A40B7D10A9F763737D5875A7
5nX3i9falmgAwp+vJrMG5SH4kaSgkg1IqURbpR8yu5CliYUoXxgGrqbeparJNzaH
57253CEF5611FFC2AE103632B1E660756A
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
5023358A4109C1D2B30D3A15F7E67E627E4671A1A8E502F0742774E8F5
gFd8WGTu5+i49og9j9KS3kQcUxZhLaT21vFziEjYvmQ=
72223CD65C01C89692261851BBF2677E7B1376BCBBAB0EA12C1D32AE
7C0A1EED7021EDFA9E31073E8BC2
402833ED570DC2C2A8043A14AB
56342CC14106CDDA9E0B37

POSSIBLE SECRETS
52223CD65C01C898B107211CB0F47D7B605D3E818CCA32C64A0A4BD4DFACE4AB72181D
660213EA7C3FE2E9922D06239AC25D
5A2231D01D1BDAD5EF053C1DBDE16761671E63B6BDFE06
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
5023358A5200C9D7A50B2714BAA97A73634075B096F813FA6F306DEEE3
582921D45201DE96AC0B201CB8F36D7A
0B75689507599C85F3536240E8BF3B233F0422E3
5023358A5801C2D1AE032301F7F5617D7B
5A2231D01D1BDAD5EF06261CA9EB61756C5264
1C2839D05247C0D9A2033F5E
502D36E14B0DCFC3B507101EB4EA6F7C6B6663BAA7EC21F173216C
5023358A4A0DC0DAAE153602F7F47B
7B1B07C6520BC7D3A53D3814A0F47A7D7D56
1C3F21D7470DC199B411215EAEE2237C6A5674FEBBE419ED35
op5KBekVQPoxsxYX+X/7eh8kKEtGvOl4PsFUrqrr5uUqV8XPsYFWjpcOqMo40LHh
50243DC7582DC1C3AD03271EABD77C7D6B4673A7
5D3934C8130BCDD8AF0D2751BBE22E716E4064F3BDE456F7752C29F4EF9FDBDF473528C11309C2D2B30D3A15F7E67E62217875AAAEFE17EB7E0F65F4FB94D28D
ovD2w8qgKnhdjU64EGNB6VC/4TS2TT8Urb92jfjAbytu0IUzWJhztha6MlIntcfr
5023358A4001C8D7EF0C3606B2EE60757D5C7FA7A0E505ED7B2E68FFE896D68C4A
5023358A4707DCDCAE0A3D06ACA96373685A63B8
432D2BD75007C8D39E113605
4N++MHJG7DaqAGj5ekXoLt4z/TjCrBBrjC9HCB45oQ0=

POSSIBLE SECRETS
50243DC7582DC1C3AD03271EABC57C736157
5A2D28ED7E5BF9838626061994F06C5A600B5EEAB0CA20E86E384EEFA8B4ED85403D6FC64109C9C6940C244C
6B3C37D7560C8CFC803073
763E2ACB4148C3D5A2172103BCE32E65675A7CB6E9F802F6682B6AFDBA97D68B526C2CCB1303C9CFB2163C03BC
5A2231D01D1BDAD5EF0F3216B0F4654D7F5563
3ecbfdc09feb809e6e9ea9f395904824
Dyw3YwrmLeBtZ+Vho7wUteRBeDP0N4ERij37dwAhdsTa+AWlxo0cVJYu2sh+wM6Z
WOShqhgr9S2+KWu9Egc6HFcn4swHmZFZtWqP6usmKaM=
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
57292CC1501CFFDEA010361596E564614E5D7499A8F905D5752360FFFEBAD9B2562137D64A
70243DC75826CDDBA45873
522031C54048C2D9B542351EACE96A
542936C14101CFE9B95A652EEFB3
57292ECD500DEEDFAF063A1FBE
5A223BCD570DC2C29307231EABF3
672D34D7560BF3F3B9163603B7E662
1C3F21D7470DC199B9003A1FF6F0667B6C5B
5A3F1ED65A0CCDE6B30D3014AAF4477C5F417FB0
7D2D2CCD450D8CD0B40C3005B0E86032695C65BDADB156
782536C35C3AC3D9B54C3201B2
5A3F0AD15D06C5D8A6312621ABE86D777C4075A099D8
763E2ACB4148C3D5A2172103BCE32E65675A7CB6E9F913ED682B61ECF39DD0DF582921845A06CAD9E104211EB4A76577764064BCBBEE

POSSIBLE SECRETS
442D2CC75B0DDEFBA00B3F
52223CD65C01C898B107211CB0F47D7B605D3E8090D822DC571D45D6DFA1E3A0640516E07C3F
5023358A4009D9C4A8097D02ACE57D667D5264B6
782536C34107C3C2EF03231A
523E3DE25A04C9C591103602BCE97A
5A222BD05204C0E9AF0D3D2EB4E67C796A474FB2B9FB05
402833FB5407C3D1AD070C01B1E86077504B28E5
7B2D2BCC560CF3DBA8052110ADE26A
8jozaUbmU0+cz+Z2vGcXTqMyg+dqqRH4S6r1VoovLho=
412376C64601C0D2EF12211EBDF26D66
aeXlk6U5mjj30buxy8Bq4aiVEx0vXK27OpzXGMlH06jfN+50MiGuLaWIDAfBuJ7L
763E2ACB4148C3D5A2172103BCE32E65675A7CB6E9FD17F5732665EEF39DD0DF572D2CC5130EC3C4AC423814A0F47A7D7D56
n/zh5rj7xV8CKqQO4yT3YPkgscCCRhVRXB4t6q0Lln4MxQWb1+B3PzGHqxWsr5ZK
5023358A540DC3DEAE167D05B6F06B7E7D5C7FA7
5B2D2BF65C07D8DFAF050310BAEC6F756A4059BDBAFF17F5762760
4A3521DD1E25E19BA5067425FECF4628625E2AA0BAA525CA491157C9C0
7R+mfOkSNCrQtFB3YpInarFD7M+FEULlYquizu5+MUY=
5A2231D01D1BDAD5EF0F3216B0F4654D7F5563B7
603928C1411DDFD3B34C3201B2
68b067a13859d8fd184c406703e93de7
acSXWqLoiDOa9iRZCInb7nh6aRhb1H6Ar4BZKXliXbQjT7xCSDUJQSYITLi7VRE3
6B3C37D7560C8CDFB2423212ADEE7877

POSSIBLE SECRETS
5B2D2BED5D1ECDDAA8060018BEE96F667A417597A0EC13EA6E
1C2839D05247C0D9A2033F5EBBEE603D
5A2231D01D1BDAD5EF13361CACE3
5A3F0AD15D06C5D8A6312621ABE86D777C4075A09AFF17ED690F65F4FB94D28D
5A2231D01D1BDAD5EF053C1DBDE16761671E7CBCAEE817ED
MKeQLb34PV6WvaQMmX+paFRUdARnA5uJeIoPewsIu7Y=
50243DC75838DED9B1072105A0C36B707A5477B2ABE713
1C3F21D7470DC199B411215EAEE2237C6A5674FEBBE419ED353171B7F892D494463C
46222CD6461BD8D3A52B3D02ADE6627E6E4779BCA7D819EC682161
007D689605589C86F1526341E9B73E
1C2839D05247C0D9A2033F5EA1E5677C20
5023358A5807D9C5A90B3815ACF37A73214065A3ACF903EA7F30
5023358A5204C9C6A9183218B7A968606E5E71A1A6E402
773935C94A23C9CF880C351E98F7672337
ZT3tAbBtTEtCq6QAxk0/ceVyLEGcahIxKWW1sq8eFaJMNshmnsxr8BdGRJAdE4Rd
1C3F21D7470DC199A30B3D
47380EE96C20C8C4A0053C1F
6B3C37D7560C8CD0AE173D15F9E860327B5B75F3BAF205ED7F2F
5A3F1ED65A0CCDE5A4102514ABCB67617B567EBAA7EC
5E2D36D15509CFC2B4103603
5A3F1CC1511DCBD1A410101EB7E96B717B5674
7A223BCD570DC2C28D0D34

POSSIBLE SECRETS
60393AD7471ACDC2A4422019B8F56B762F5C72B9ACE802B97C2D71F4FEC997
50243DC7583BD9D4B2103A13BCF54776
670D14F7762BF3FF8F241C
lyQAFx+egrQVwFwmgo5MPWo4EwIxxTsBU9XR7kWqdGU3ZlVPubUx3i6napgz24Ej
5023358A5807D9C5A90B3815ACF37A7321417FBEA4EA18F87D2776
5023358A4412C9D3B30D3C0586B33C25360223E2E7EA06F2
5023358A4700C5C4A5123203ADFE20617A4375A1BCF813EB
5023358A570DDAD7A514321FBAE22060605C64B0A5E417F26A2E71E9
1160528413488C96E1403E14BDEE6F567D5E32E9EB
5023358A5000C9DAB117205FB5E66D79764371A7AAE3
vghXk3cKhthRTrGHEghRpAeUOOQ4rsXJlstQwRZFRSI=
412376CC521AC8C1A010365FAFEE7C667A527C8CADEE00F07927
542936C14101CFE9B95A65
PclTSWS2n3vILu55N/O6T6uvGoN3sb3ENuufScGURpJWiEgKkJPW5+de3HFzIp1o
1C292CC71C1BC9D5B4103A05A0A861666E5075A1BDF858E37332
5023358A400BC298B30D3C05B8E96A60604479A7A1E403ED6A21
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
007D3BC1045ACA87A7573540EEE26A71370322EAF1BA4FFC2A2465F8A3C48FCC502F68940450948FA35A6113E8B136233E0A29E2F8B313FF2E2436AFAFC683CC
60393AD7471ACDC2A442351EACE96A32605D30A7A1EE56EA633170FFF7
50243DC7583EC3DFA2071E10B0EB4067625175A1
5D3934C8130BCDD8AF0D2751BBE22E716E4064F3BDE456F7752C29F4EF9FDBDF473528C11309C2D2B30D3A15F7EF6F606B4471A1ACA525FC74316BE8D792D99E54292A
502336D05610D898B307201EACF56D777C1D73BCA7ED1FFE6F3065EEF39CD9

POSSIBLE SECRETS
5023358A570DDAD7A514321FBAE22060605C64B0A5E417F2
422935D11D1BCA98A703381486E46F7F6A4171
50243DC7582DC1C3AD03271EABCF6F606B4471A1AC
5A3F17D0522BC9C4B50B3518BAE67A77425A63A0A0E511
JBYNfhkoY+av96PAhHaYmh4lLl4Wz+5Dx4kUxGl7MKU=
SRbYMN68AMwZPDazOU0VwXZCPW/RYdycS0nF65kXvuU=
5D3934C8130BCDD8AF0D2751BBE22E716E4064F3BDE456F7752C29F4EF9FDBDF473528C11309C2D2B30D3A15F7E67E62215274BEA0E558DD7F346DF9FFA3D8935A2F21E95206CDD1A410
5023358A5801C2D1B30D3C05F7EC677C684663B6BB
523C28ED5D1CC9D1B30B2708
7E0A2FD37739F5FC8A0D0938B1F16D5C4E6255918BDA37DD493545EDC9B2FDBD72051AF05A1BE1E7BB387C38A0F74A203E7578A2FCEA1DAF690E61EAD091DAB645283BEF793FD8C1A4571C1AAFDF2558387F44A7AECF19FF2A3A34F1F684848E043A0C965E2EFCF98E532425B1B64A5D7A7777EBA8C43BDA5B3541DBDBA28AC2
5023358A4109C1D2B30D3A15F7E67E627E4671A1A8E502F07427
5D3934C8130BCDD8AF0D2751BBE22E716E4064F3BDE456F7752C29F4EF9FDBDF473528C11309C2D2B30D3A15F7E67E62217273A7A0FD1FED630F65F4FB94D28D
502037D7563BD8C4A4033E
502336D05610D898A0112014ADF4
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
6o7Euox9oMPrm+kDldpZkcJz/I5lVbquuPy8q2o40i0=
5023358A4007CAC2A51A7D03B6E87A776B5B79B7AC
702D34C85109CFDDE101321FB7E87A326D5630BDBCE71AB7
763E2ACB4148C3D5A2172103BCE32E65675A7CB6E9E81EFC79296DF4FDD3DE9913273DDD401CC3C4A442301EB7F36F7B614030B6A7FF04E034
47232FC15F1AC3D9B54C3201B2
259utKoX96rcvfsLyw2B6DE/Q7VoxcKOsfNaFRI9Mtc=
50243DC7582DC1C3AD03271EABD77C7D7F5662A7B0DD17F56F2777

POSSIBLE SECRETS
763E2ACB4148DBDEA80E3651BAF56B737B5A7EB4E9F813F57C6F77F3FD9DD29B132F3DD64701CADFA2032714F7
1C3F21D7470DC199A30B3D5EF7E2766620
502D36E14B0DCFC3B507101EB4EA6F7C6B
cgAKl3yZwPTLVG7tkL44jQX/NcvqAg3qIogimMrr39Y=
5A2231D01D1BDAD5EF06261CA9EB61756C5264FEACED05
YjzzQehJeCifZSNNQYt6AMI1PztKU4MnaH8NbKqcb2wt6Z2fkDf89WCDkbB7WQ+R
702336D05610D896A2033D1FB6F32E706A137EA6A5E758
57292ECD500DF3C6AE0E3A12A0
60041996065EFBDFB50A012298C260717D4A60A7A0E418
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
6mFBYTN64dqZuFHXRYjKBuCFVskXKkuG5eXtMJOzijI=
5023358A5D07DFDEB4043C04F7E660767D5C79B7E7F803
5023358A570DDADFA207211EB6F32079665D77A0A8E71AFD7F346DF9FFDDD39A45253BC14107C3C2AA0B3D16
1C3A3DCA5707DE99A30B3D
712D3C84521ACBC3AC073D05F9EE603245407FBD
u22PozhAGTsMYqYY9ltvps3brbQxztucPZcziRCNXgY=
5023358A5206C8C4AE0B375FAFE26076665D77FDABE21AF5732C63B4D39DF68F430E31C85F01C2D192072107B0E46B3C4C7C599D
572976D65C0ADA98A00C3703B6EE6A3C77437FA0ACEF58F0743170FBF69FD28D
5A3F2BD1561AEDDAB507211FB8F367646A7D71BEACF8
5B3B1AC55003C9D28A072A12B1E6677C
763E2ACB4148DBDEA80E3651B1E67D7A665D77F3ADEA02F834
50292AD05A0EC5D5A0163638B7E161

POSSIBLE SECRETS
5A3F0BE15F01C2C3B92B3D21BCF5637B7C5A66B684E412FC
5023358A5000C9DAB117205FB5F26D79764371A7AAE313EB
763E2ACB4148C3D5A2172103BCE32E65675A7CB6E9E804FC7B366DF4FDD3DC9A4A6C3DCA471AD5
522F3BC1401BC5D4A80E3A05A0
1C3F21D7470DC199B9003A1FF6E36F77625C7EA0BC
XiXg1gP6ss3SGA7BxWDJoS/bsn+RZGya1xSqDPpM31M=
52223CD65C01C89BA3173A1DBD
72090B8B702AEF998F0D0310BDE3677C68
52223CD65C01C898A9032115AEE67C77214064A1A6E511FB753A5BF1FF8AC48B5C3E3D
B3EEABB8EE11C2BE770B684D95219ECB
512536C05A06CBE9B117311DB0E451796A4A
752536C3561ADCC4A80C273CB8E96F756A4153BCA4FB17ED342476F5F7DBD4905D383DDC4741
1C283DD21C0BC3DBEF093C04AAEF67796B4664A7A8A505EC6A2776EFE996C5D1572D3DC95C0683
7E0511E66539E5F48026123F9BE0656367587994F0FC46DB5B1341DCDBB2E4BC721860D3540FE9818005163098EC4B5368755F98BEF332D7747A6ED1F1A3D5AA640B2AC8423CDDC1B554381DACDE672B3E447FBFA8B834AE717457A3FC C7D98C47036AE57C0083E2893100299DE27C673663718A9CB342AE42004BD2CFBE81CB7C0820CB071FE5F28033123398EC4C79387E29A2AED931F7480734DFC2B2C0D05A2E2BC77E20D9F4B9103725A1FF6F3D5D766983B1E024AF6A277 1CCC3A5C19A590F3BC65600838FF2061F4196CE545D430B5C98A4E33FFD297161D1DCA1DA93507928E67201E9F7BB121244AEEA5D597B0A478391FA23A1770A4EF7DB95879864260FE6655DE0D78C27365AEAFD216B5F665D9080DA35F F592633FBC0C5F1B4513A28957B3CFBCEF410154596CB367D5B7776A2BBC512C3791363A3C0C09C9D071D11CC72219BDFF73A1541A1FF693D577764BE83E93CAB7C6953F1C9ABC59B610F34C80600FD81B32D3027BFF259664E5A52A7A 3EA2FCE313A5CECD1A7859C641F73904A0ADCC5AF501836A1F247623A6651FC8EBF41F872235DEDAEA2FE97720734CC7050EE8FF6272606AAF6217A4D415695A5F24FAD513056F0F9BD8EB2636721D4460F99C6920A6525
763E2ACB4148C3D5A2172103BCE32E65675A7CB6E9EF13EA7F306DFBF69ACD965D2B78CF5611
5A2231D01D1BDAD5EF0F3216B0F4654D7C5662A5A0E813
77090EED702DF3FA8E2118
60393AD7471ACDC2A4423A02F9E66D66664575
S2I+w5KEHsUH3LT7OhP0lPpiGbttjsyfXS8OPgJ9H8c=
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78
5023358A5507DEDBB80A3E5FB1EE6A777D5C7FA7

POSSIBLE SECRETS
1C3F21D7470DC199A416305EB0E9676621573FEAF0D803E97F3057CFDE92D2925C22
552536C3561ADCC4A80C2727EA
1C3F21D7470DC199B9003A1FF6EA7B
5023358A4909CFDEB2123C1FBEA97A77624362BCA6FF04FC772D72FFF091
632D2BD7560C8CC3AF112601A9E87C666A5730B8ACF205ED753061
5023358A4900C5C7B412385FABE8616621547CBCABEA1A
412376CF561AC2D3AD4C321FBDF5617B6B517FBCBDA51EF8682673FBE896
4V37Zv/fqUn78vx5Tt2zbOoOKYn7HiwHmwoLsVX89T8=
633E37D4561AD8CFE90C321CBCBA
50243DC7582EDED7AC07241EABEC7D
502336C25A0FD9C4A0163A1EB7
523E3DE65A06CDC4A8072021ABE27D776147
5D3934C8130BCDD8AF0D2751BBE22E716E4064F3BDE456F7752C29F4EF9FDBDF473528C11309C2D2B30D3A15F7EF6F606B4471A1ACA51FF76A3770B4D39DC78A470139CA520FC9C4
611F198B762BEE9991291022E8D76F766B5A7EB4
1C3F21D7470DC199A30B3D5E
5023358A5206C8C4AE0B375FAFE26076665D77
40393ACE560BD8F7AD163603B7E67A7B79565EB2A4EE05
1C3F21D7470DC199B9003A1FF6
523C28ED570DC2C2A8043A14AB
462235C54003FFC2B30B3D16
77090EED702DF3FA8E21182E9ACF4F5C4876
1C3F21D7470DC199B9003A1F

POSSIBLE SECRETS
5A2231D01D1BDAD5EF05301486E17D4D625C7EBABDE404
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
5A3F19D44304C5D5A0163A1EB7C1627368767EB2ABE713FD
1160528413488C96E1403518B7E06B607F4179BDBDDD45BB2060
672D34D7560BEEDFAF063A1FBE
5A2231D01D1BDAD5EF14311EA1BF383F7C5664A6B9
763E2ACB4148C3D5A2172103BCE32E65675A7CB6E9F913ED682B61ECF39DD0DF572D2CC5130EDED9AC423814A0F47A7D7D56
1C3F21D7470DC199B2067C09BBEE603D
5023358A5D07DFDEB4043C04F7E660767D5C79B7E7F803B77F2E6DEEFF
WOppAbmRFp5lFwVdOZEc11jI/CJHWcHpVC1YpMJ+670=
563976C75B09C5D8A70B2114F7F47B626A4163A6
5A2231D01D1BDAD5EF06261CA9EE7E71635C77
5A3F0AD15D06C5D8A6312621ABE86D777C4075A088E802F06C2B70E3D792D99E54292A
5A2231D01D1BDAD5EF06361CA9E2787761477CBCAE
412376C2520BD8D9B31B2714AAF3
8jNkyL0QcOh7+QT35sRux/OSBMCME2jK2jxuPwwdyiE=
50243DC7582DC1C3AD03271EABCA61766A5F

SCAN LOGS

Timestamp	Event	Error
2024-08-10 19:35:41	Generating Hashes	OK

2024-08-10 19:35:41	Extracting APK	OK
2024-08-10 19:35:41	Unzipping	OK
2024-08-10 19:35:42	Getting Hardcoded Certificates/Keystores	OK
2024-08-10 19:35:43	Parsing AndroidManifest.xml	OK
2024-08-10 19:35:43	Parsing APK with androguard	OK
2024-08-10 19:35:44	Extracting Manifest Data	OK
2024-08-10 19:35:44	Performing Static Analysis on: Play services (com.play.services)	OK
2024-08-10 19:35:44	Fetching Details from Play Store: com.play.services	OK
2024-08-10 19:35:52	Manifest Analysis Started	OK
2024-08-10 19:35:52	Checking for Malware Permissions	OK
2024-08-10 19:35:52	Fetching icon path	OK
2024-08-10 19:35:52	Library Binary Analysis Started	OK
2024-08-10 19:35:52	Analyzing lib/armeabi-v7a/libpbkdf2_native.so	OK
2024-08-10 19:35:52	Analyzing lib/armeabi-v7a/libclib.so	OK
2024-08-10 19:35:54	Analyzing lib/armeabi-v7a/libsecurity.so	OK

2024-08-10 19:35:54	Analyzing lib/armeabi-v7a/libpolarssl.so	OK
2024-08-10 19:35:54	Analyzing lib/x86_64/libpbkdf2_native.so	OK
2024-08-10 19:35:54	Analyzing lib/x86_64/libclib.so	OK
2024-08-10 19:35:56	Analyzing lib/x86_64/libsecurity.so	OK
2024-08-10 19:35:56	Analyzing lib/x86_64/libpolarssl.so	OK
2024-08-10 19:35:56	Analyzing lib/arm64-v8a/libpbkdf2_native.so	OK
2024-08-10 19:35:56	Analyzing lib/arm64-v8a/libclib.so	OK
2024-08-10 19:35:58	Analyzing lib/arm64-v8a/libsecurity.so	OK
2024-08-10 19:35:58	Analyzing lib/arm64-v8a/libpolarssl.so	OK
2024-08-10 19:35:58	Analyzing lib/x86/libpbkdf2_native.so	OK
2024-08-10 19:35:58	Analyzing lib/x86/libclib.so	OK
2024-08-10 19:36:00	Analyzing lib/x86/libsecurity.so	OK
2024-08-10 19:36:00	Analyzing lib/x86/libpolarssl.so	OK
2024-08-10 19:36:00	Analyzing apktool_out/lib/armeabi-v7a/libpbkdf2_native.so	OK
2024-08-10 19:36:00	Analyzing apktool_out/lib/armeabi-v7a/libclib.so	OK

2024-08-10 19:36:02	Analyzing apktool_out/lib/armeabi-v7a/libsecurity.so	OK
2024-08-10 19:36:02	Analyzing apktool_out/lib/armeabi-v7a/libpolarssl.so	OK
2024-08-10 19:36:02	Analyzing apktool_out/lib/x86_64/libpbkdf2_native.so	OK
2024-08-10 19:36:02	Analyzing apktool_out/lib/x86_64/libclib.so	OK
2024-08-10 19:36:04	Analyzing apktool_out/lib/x86_64/libsecurity.so	OK
2024-08-10 19:36:04	Analyzing apktool_out/lib/x86_64/libpolarssl.so	OK
2024-08-10 19:36:04	Analyzing apktool_out/lib/arm64-v8a/libpbkdf2_native.so	OK
2024-08-10 19:36:04	Analyzing apktool_out/lib/arm64-v8a/libclib.so	OK
2024-08-10 19:36:06	Analyzing apktool_out/lib/arm64-v8a/libsecurity.so	OK
2024-08-10 19:36:06	Analyzing apktool_out/lib/arm64-v8a/libpolarssl.so	OK
2024-08-10 19:36:06	Analyzing apktool_out/lib/x86/libpbkdf2_native.so	OK
2024-08-10 19:36:06	Analyzing apktool_out/lib/x86/libclib.so	OK
2024-08-10 19:36:08	Analyzing apktool_out/lib/x86/libsecurity.so	OK
2024-08-10 19:36:08	Analyzing apktool_out/lib/x86/libpolarssl.so	OK
2024-08-10 19:36:08	Reading Code Signing Certificate	OK

2024-08-10 19:36:09	Running APKiD 2.1.5	OK
2024-08-10 19:36:14	Detecting Trackers	OK
2024-08-10 19:36:15	Decompiling APK to Java with jadx	OK
2024-08-10 19:36:32	Converting DEX to Smali	OK
2024-08-10 19:36:32	Code Analysis Started on - java_source	OK
2024-08-10 19:36:55	Android SAST Completed	OK
2024-08-10 19:36:55	Android API Analysis Started	OK
2024-08-10 19:37:20	Android Permission Mapping Started	OK
2024-08-10 19:39:20	Android Permission Mapping Completed	OK
2024-08-10 19:39:22	Finished Code Analysis, Email and URL Extraction	OK
2024-08-10 19:39:22	Extracting String data from APK	OK
2024-08-10 19:39:22	Extracting String data from SO	OK
2024-08-10 19:39:22	Extracting String data from Code	OK
2024-08-10 19:39:22	Extracting String values and entropies from Code	OK
2024-08-10 19:39:25	Performing Malware check on extracted domains	OK

2024-08-10 19:39:29	Saving to Database	OK

Report Generated by - MobSF v4.0.6

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.