MOBSF

ANDROID STATIC ANALYSIS REPORT

Ovia (6.18.0)

File Name: com.ovuline.fertility_13587.apk

Package Name:	com.ovuline.fertility
Scan Date:	Sept. 1, 2025, 6:57 a.m.
App Security Score:	48/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	7/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	25	3	2	1

FILE INFORMATION

File Name: com.ovuline.fertility_13587.apk
Size: 25.5MB
MD5: 7292a027152ffd85fc5eb99eeb0f5ad4
SHA1: f13f1b413c2239fe225c3622c386e8bc6dd3c2aa
SHA256: 902a11bf54c10f1365683eb01650abf66506cb759ddc1effe0c225d5b41a6425

APP INFORMATION

App Name: Ovia
Package Name: com.ovuline.fertility
Main Activity: com.ovuline.fertility.ui.activities.SplashActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 6.18.0
Android Version Code: 13587

APP COMPONENTS

Activities: 50
Services: 13
Receivers: 14

Providers: 8
Exported Activities: 5
Exported Services: 2
Exported Receivers: 5
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=US, ST=MA, L=Boston, O=Ovuline, OU=Android team, CN=Vyacheslav Boychenko
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-09-15 11:51:58+00:00
Valid To: 2039-09-09 11:51:58+00:00
Issuer: C=US, ST=MA, L=Boston, O=Ovuline, OU=Android team, CN=Vyacheslav Boychenko
Serial Number: 0x5416d2de
Hash Algorithm: sha1
md5: ec665c603807816fa82a058c07dff3ee
sha1: 9f39a79e8faea73b315777b3fad57b6926317f96
sha256: 62ad57df2a5ede7d417cf2d390129bf1c4e621d6b0ffea3668b99708cb234d5e
sha512: 712194de8280ebc19ad533b99f6dd0f3aa217593730faebb31aea59e28a72f765fd4171fa1e3e3651dbcbcc4d0296fab57ea16c3260be2a7dae6f0479e77d029
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: c6a373c687ac0dc178c6cdce0c22be6894a5627157ac24ec0d0071ccdaeca87c
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.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.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.
com.ovuline.fertility.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.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.BOARD check
network operator name check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.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
ro.kernel.qemu check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.TAGS check
possible ro.secure check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes5.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</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.ovuline.fertility.ui.activities.IntentFilterActivity	Schemes: oviafertility://, https://, Hosts: update, delete, timeline, timeline-rate-app, rate-app, parenting-app, preg-app, webview, custom-tab, support, support-faq, call, devices, deals, myq, data-entry, settings, color-themes, messaging, report-pregnancy, calendar, cycle-insights, chart, articles, insurance-entry, healthcare-info, provider-info, doctor-info, community, special-conditions, contact-provider, native-health, profile, checklist, birth-control-setup, video, videos, birth-control-profile, health-pathways, ovia-plus, first-dollar, open, cvs-minute-clinic, oviahealth.onelink.me, Path Prefixes: /gZn1,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 14 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Activity (com.ovuline.fertility.ui.activities.IntentFilterActivity) 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.
4	Broadcast Receiver (com.ovuline.ovia.receiver.OnLocaleChangedReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Broadcast Receiver (com.ovuline.ovia.receiver.OnAppUpgradeReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Service (androidx.work.impl.background.systemjob.SystemJobService) 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.
7	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	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.
9	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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.
10	Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
11	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **2** | WARNING: **9** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				N1/a.java b7/C0183d.java b7/C1305d.java b7/k.java b7/r.java b7/s.java coil/memory/MemoryCache.java com/amazonaws/auth/CognitoCachingCredentialsProvi der.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				der.java com/amazonaws/auth/policy/conditions/ConditionFactory.java com/amazonaws/auth/policy/conditions/S3ConditionFactory.java com/amazonaws/cognito/clientcontext/data/UserContextDataProvider.java com/amazonaws/cognito/clientcontext/datacollection/DeviceDataCollector.java com/amazonaws/internal/keyvaluestore/AWSKeyValueStore.java com/amazonaws/internal/keyvaluestore/KeyProvider18.java com/amazonaws/mobile/auth/core/IdentityManager.java com/amazonaws/mobile/auth/userpools/CognitoUserPoolsSignInProvider.java com/amazonaws/mobile/client/AWSMobileClient.java com/amazonaws/mobile/client/internal/oauth2/OAuth2Client.java com/amazonaws/mobileconnectors/cognitoidentityprovider/util/CognitoDeviceHelper.java com/amazonaws/mobileconnectors/cognitoidentityprovider/util/CognitoPinpointSharedContext.java com/amazonaws/mobileconnectors/cognitoidentityprovider/util/CognitoServiceConstants.java com/amazonaws/mobileconnectors/s3/transferutility/TransferObserver.java com/amazonaws/mobileconnectors/s3/transferutility/TransferTable.java com/amazonaws/services/s3/Headers.java com/amazonaws/services/s3/model/S3ObjectSummary.java com/amplifyframework/analytics/pinpoint/AWSPinpointAnalyticsPlugin.java com/amplifyframework/auth/AWSTemporaryCredentials.java com/amplifyframework/auth/AuthProvider.java com/amplifyframework/auth/AuthUser.java com/amplifyframework/auth/AuthUserAttribute.java com/amplifyframework/auth/AuthUserAttributeKey.java com/amplifyframework/auth/TOTPSetupDetails.java com/amplifyframework/auth/cognito/AWSCognitoAuthPlugin.java com/amplifyframework/auth/cognito/AuthEnvironment

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	.java com/amplifyframework/auth/cognito/actions/DeviceSRPCognitoSignInActions.java com/amplifyframework/auth/cognito/actions/FetchAuthSessionCognitoActions.java com/amplifyframework/auth/cognito/actions/MigrateAuthCognitoActions.java com/amplifyframework/auth/cognito/actions/SRPCognitoActions.java com/amplifyframework/auth/cognito/actions/SetupTOTPCognitoActions.java com/amplifyframework/auth/cognito/actions/SignInChallengeCognitoActions.java com/amplifyframework/auth/cognito/actions/SignInCustomCognitoActions.java com/amplifyframework/auth/cognito/activities/CustomTabsManagerActivity.java com/amplifyframework/auth/cognito/asf/DeviceDataCollector.java com/amplifyframework/auth/cognito/asf/UserContextDataProvider.java com/amplifyframework/auth/cognito/data/AWSCognitoLegacyCredentialStore.java com/amplifyframework/auth/plugins/core/data/AWSCredentialsInternal.java com/amplifyframework/core/category/CategoryConfiguration.java com/amplifyframework/pinpoint/core/TargetingClient.java com/amplifyframework/pinpoint/core/util/SharedPreferencesUtilKt.java com/amplifyframework/statemachine/codegen/data/AWSCredentials.java com/amplifyframework/statemachine/codegen/data/AuthChallenge.java com/amplifyframework/statemachine/codegen/data/CredentialType.java com/amplifyframework/statemachine/codegen/data/DeviceMetadata.java com/amplifyframework/statemachine/codegen/data/OauthConfiguration.java com/amplifyframework/statemachine/codegen/data/SignInData.java com/amplifyframework/statemachine/codegen/data/SignInTOTPSetupData.java com/amplifyframework/statemachine/codegen/data/Si

NO	ISSUE	SEVERITY	STANDARDS	FILES
				gnedInData.java com/amplifyframework/statemachine/codegen/data/SignedOutData.java com/amplifyframework/statemachine/codegen/data/UserPoolConfiguration.java com/amplifyframework/statemachine/codegen/events/CustomSignInEvent.java com/amplifyframework/statemachine/codegen/events/DeviceSRPSignInEvent.java com/amplifyframework/statemachine/codegen/events/SRPEvent.java com/amplifyframework/statemachine/codegen/events/SetupTOTPEvent.java com/amplifyframework/statemachine/codegen/events/SignInEvent.java com/amplifyframework/statemachine/codegen/states/SetupTOTPState.java com/amplifyframework/storage/StorageItem.java com/apptentive/android/sdk/conversation/LegacyConversationMetadataItem.java com/apptentive/android/sdk/encryption/resolvers/KeyResolver18.java com/bumptech/glide/load/engine/c.java com/bumptech/glide/load/engine/m.java com/bumptech/glide/load/engine/r.java com/ovia/dlp/data/repository/VaginalBleedingAmount.java com/ovia/dlp/data/repository/VaginalBleedingColor.java com/ovia/dlp/data/repository/VaginalClots.java com/ovia/dlp/data/repository/VaginalOdor.java com/ovuline/ovia/data/network/update/UserAuthenticationInfo.java com/ovuline/ovia/network/IOviaRestService.java d7/C0375a.java d7/C1545a.java h1/C0224i.java h1/C1653i.java s1/C0266a.java s1/C2257a.java v2/C0074c.java v2/C2333c.java w1/C0295k.java w1/C0305v.java w1/C2371k.java w1/C2381v.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				w1/L.java w1/Z.java
2	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	C6/a.java F7/a.java V4/a.java com/ovuline/ovia/network/OviaNetworkCommonModule.java com/ovuline/ovia/network/OviaNetworkRetrofitModule.java j9/g.java j9/h.java j9/m.java j9/n.java
				A2/e.java A2/i.java B2/a.java C2/c.java C2/d.java C2/f.java C2/r.java C2/s.java E2/d.java I2/a.java I2/d.java I2/j.java K2/e.java K2/f.java K2/k.java K2/l.java K2/n.java K2/o.java L2/d.java N2/b.java R2/a.java T/c.java T/l.java Y7/f.java b3/AbstractC1294a.java b3/a.java com/amazonaws/logging/AndroidLog.java com/amplifyframework/logging/JavaLogger.java com/amplifyframework/statemachine/StateMachine$sp

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	ecial$$inlined$CoroutineExceptionHandler$1.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1qSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1jSDK.java com/appsflyer/internal/AFf1kSDK.java com/apptentive/android/sdk/conversation/LegacyConversationMetadata.java com/bumptech/glide/b.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/g.java com/bumptech/glide/load/engine/h.java com/bumptech/glide/load/engine/t.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/c.java com/bumptech/glide/load/resource/bitmap/e.java com/bumptech/glide/load/resource/bitmap/j.java com/bumptech/glide/load/resource/bitmap/k.java com/bumptech/glide/load/resource/bitmap/o.java com/bumptech/glide/load/resource/bitmap/v.java com/bumptech/glide/load/resource/bitmap/y.java com/bumptech/glide/request/SingleRequest.java io/sentry/android/core/C0107t.java io/sentry/android/core/C1751t.java io/sentry/android/core/p0.java io/sentry/c2.java k9/e.java l3/C0478i.java l3/C2017i.java org/slf4j/helpers/l.java t2/C0067a.java t2/C2276a.java u2/d.java u2/e.java w2/AbstractC0080b.java w2/AbstractC2387b.java w2/j.java w2/l.java x2/C0083c.java x2/C0085e.java x2/C2414e.java z2/i.java z2/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	b7/p.java com/amazonaws/mobileconnectors/s3/transferutility/TransferTable.java com/amplifyframework/pinpoint/core/database/EventTable.java com/amplifyframework/pinpoint/core/database/PinpointDatabaseHelper.java f3/M.java f3/U.java io/sentry/android/sqlite/SentrySupportSQLiteDatabase.java
5	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/amplifyframework/devmenu/DeveloperMenu.java com/ovia/branding/theme/views/ViewsKt.java com/ovia/coaching/ui/conversation/ConversationFragment.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/github/mikephil/charting/BuildConfig.java
7	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	H1/d.java P3/a.java io/sentry/util/t.java
8	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	coil/decode/K.java com/amazonaws/mobileconnectors/s3/transferutility/TransferUtility.java com/ovuline/ovia/utils/FileStorageUtils.java
9	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	B7/f.java com/amazonaws/services/s3/internal/MD5DigestCalculatingInputStream.java com/amazonaws/util/Md5Utils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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	N8/a.java com/amazonaws/retry/PredefinedRetryPolicies.java com/appsflyer/internal/AFa1zSDK.java com/appsflyer/internal/AFb1hSDK.java com/appsflyer/internal/AFc1fSDK.java
11	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	R7/a.java io/sentry/android/core/internal/util/k.java
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	R7/b.java io/sentry/android/core/internal/util/k.java l3/v.java
13	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	B7/f.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/utils/FileUtils.java com/ovuline/ovia/utils/B.java com/ovuline/ovia/utils/FileStorageUtils.java io/sentry/android/core/X.java
14	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	Q0/b.java
15	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/appsflyer/internal/AFb1vSDK.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	arm64-v8a/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	x86_64/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	x86_64/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	x86_64/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86_64/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	armeabi-v7a/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	armeabi-v7a/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	armeabi-v7a/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	armeabi-v7a/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	x86/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	x86/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	x86/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	x86/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	arm64-v8a/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	arm64-v8a/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	arm64-v8a/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	arm64-v8a/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	x86_64/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	x86_64/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	x86_64/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	x86_64/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	armeabi-v7a/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	armeabi-v7a/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
27	armeabi-v7a/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	armeabi-v7a/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	x86/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
30	x86/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	x86/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	x86/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	P7/c.java b7/k.java com/amazonaws/mobile/client/AWSMobileClient.java com/amplifyframework/auth/cognito/helpers/BrowserHelper.java com/amplifyframework/devmenu/DevMenuFileIssueFragment.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1cSDK.java com/appsflyer/internal/AFc1jSDK.java com/appsflyer/internal/AFf1sSDK.java com/ovia/checklists/c.java com/ovia/coaching/ui/conversation/ConversationFragment.java com/ovia/health/ui/MyOviaPlusFragment.java com/ovia/healthintegrations/DeviceInfoFragment.java com/ovia/pregnancy/ui/fragment/entries/AddEntryFragment.java com/ovia/pregnancybyweek/ui/InTheWombViewerActivity.java com/ovuline/fertility/ui/activities/IntentFilterActivity.java com/ovuline/ovia/services/gcm/LocalNotificationSchedulerService.java com/ovuline/ovia/timeline/mvp/BaseTimelinePresenter.java com/ovuline/ovia/ui/activity/BaseIntentFilterActivity.java com/ovuline/ovia/ui/activity/BaseSplashActivity.java com/ovuline/ovia/ui/dialogs/o.java com/ovuline/ovia/utils/B.java com/ovuline/ovia/utils/FileStorageUtils.java com/ovuline/ovia/utils/z.java g4/C0398d.java g4/C0399e.java g4/C1622d.java g4/C1623e.java l4/c.java n3/C0494a.java n3/C2074a.java r4/AbstractC0556b.java r4/AbstractC2241b.java w7/AbstractC0602a.java
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1jSDK.java com/helpshift/activities/HSMainActivity.java com/ovuline/ovia/ui/activity/BaseSplashActivity.java com/ovuline/ovia/ui/fragment/profile/BaseProfileFragment.java o7/AbstractC0512b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	coil/disk/a.java com/amazonaws/auth/PropertiesCredentials.java com/amazonaws/mobileconnectors/s3/transferutility/TransferDBUtil.java com/amazonaws/mobileconnectors/s3/transferutility/TransferObserver.java com/amazonaws/services/s3/internal/ServiceUtils.java com/appsflyer/internal/AFg1nSDK.java com/apptentive/android/sdk/conversation/LegacyConversationMetadataItem.java com/github/mikephil/charting/charts/Chart.java com/helpshift/log/b.java com/ovuline/ovia/utils/FileStorageUtils.java e7/C0383a.java e7/C0384b.java e7/C1563a.java e7/C1564b.java io/sentry/AbstractC0153o.java io/sentry/AbstractC1797o.java io/sentry/C0173v.java io/sentry/D0.java io/sentry/F0.java io/sentry/SentryOptions.java io/sentry/android/core/AbstractC0112y.java io/sentry/android/core/X.java io/sentry/android/core/cache/b.java io/sentry/cache/b.java io/sentry/cache/c.java io/sentry/cache/e.java io/sentry/instrumentation/file/a.java o2/f.java o2/g.java o4/C0509c.java o4/C2102c.java x4/e.java
00096	Connect to a URL and set request method	command network	com/amazonaws/http/UrlHttpClient.java com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java o2/C2096b.java o2/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/amazonaws/http/UrlHttpClient.java com/amazonaws/util/HttpUtils.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java w2/j.java
00109	Connect to a URL and get the response code	network command	com/amazonaws/http/UrlHttpClient.java com/amazonaws/util/HttpUtils.java com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/appsflyer/internal/AFf1oSDK.java w2/j.java
00036	Get resource file from res/raw directory	reflection	a2/C0593e.java a2/e.java com/amazonaws/mobileconnectors/s3/transferutility/TransferDBBase.java com/amplifyframework/pinpoint/core/database/PinpointDatabase.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFi1mSDK.java com/appsflyer/internal/AFi1sSDK.java com/ovuline/ovia/utils/FileStorageUtils.java n3/C0494a.java n3/C2074a.java r4/AbstractC0556b.java r4/AbstractC2241b.java w7/AbstractC0602a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	B0/b.java B7/a.java B7/f.java C2/f.java Y7/e.java com/amazonaws/auth/PropertiesCredentials.java com/amazonaws/internal/ReleasableInputStream.java com/amazonaws/internal/ResettableInputStream.java com/amazonaws/regions/RegionUtils.java com/amazonaws/services/s3/internal/RepeatableFileInputStream.java com/amazonaws/services/s3/internal/ServiceUtils.java com/amazonaws/util/Md5Utils.java com/appsflyer/internal/AFb1iSDK.java com/appsflyer/internal/AFg1nSDK.java com/apptentive/android/sdk/serialization/ObjectSerialization.java com/apptentive/android/sdk/storage/FileSerializer.java com/apptentive/android/sdk/util/Util.java com/bumptech/glide/load/a.java f4/d.java io/sentry/C0173v.java io/sentry/C0181x1.java io/sentry/D0.java io/sentry/F0.java io/sentry/cache/b.java io/sentry/cache/c.java io/sentry/cache/e.java io/sentry/config/e.java io/sentry/instrumentation/file/b.java io/sentry/instrumentation/file/h.java o2/f.java o2/g.java o9/w.java t2/C0067a.java t2/C2276a.java x4/e.java
00202	Make a phone call	control	com/ovuline/ovia/ui/activity/BaseIntentFilterActivity.java com/ovuline/ovia/ui/dialogs/o.java l4/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00203	Put a phone number into an intent	control	com/ovuline/ovia/ui/activity/BaseIntentFilterActivity.java com/ovuline/ovia/ui/dialogs/o.java l4/c.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/ovuline/ovia/services/gcm/LocalNotificationSchedulerService.java com/ovuline/ovia/ui/activity/BaseIntentFilterActivity.java com/ovuline/ovia/ui/activity/BaseSplashActivity.java com/ovuline/ovia/ui/dialogs/o.java l4/c.java
00016	Get location info of the device and put it to JSON object	location collection	com/ovuline/ovia/data/network/update/TrackLocationUpdate.java
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFi1mSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1qSDK.java
00012	Read data and put it into a buffer stream	file	B7/a.java com/amazonaws/util/Md5Utils.java f4/d.java io/sentry/C0173v.java io/sentry/C0181x1.java io/sentry/D0.java io/sentry/cache/b.java io/sentry/cache/e.java io/sentry/config/e.java
00014	Read file into a stream and put it into a JSON object	file	com/appsflyer/internal/AFg1nSDK.java f4/d.java
00004	Get filename and put it to JSON object	file collection	f4/d.java
00094	Connect to a URL and read data from it	command network	com/amazonaws/http/UrlHttpClient.java
00108	Read the input stream from given URL	network command	com/amazonaws/http/UrlHttpClient.java

RULE ID	BEHAVIOUR	LABEL	FILES
00192	Get messages in the SMS inbox	sms	com/amazonaws/mobileconnectors/s3/transferutility/TransferDBUtil.java com/appsflyer/internal/AFb1jSDK.java com/ovuline/ovia/utils/FileStorageUtils.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/ovuline/ovia/utils/FileStorageUtils.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1sSDK.java com/ovuline/ovia/utils/FileStorageUtils.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1sSDK.java com/ovuline/ovia/utils/FileStorageUtils.java x2/C0083c.java
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFg1nSDK.java o4/C0509c.java o4/C2102c.java
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFi1oSDK.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFi1oSDK.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFi1oSDK.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFi1oSDK.java
00030	Connect to the remote server through the given URL	network	com/appsflyer/internal/AFb1uSDK.java o2/C2096b.java o2/b.java w2/j.java

RULE ID	BEHAVIOUR	LABEL	FILES
00065	Get the country code of the SIM card provider	collection	com/ovuline/ovia/utils/B.java j4/C0440d.java j4/C1845d.java
00132	Query The ISO country code	telephony collection	com/ovuline/ovia/utils/B.java
00162	Create InetSocketAddress object and connecting to it	socket	j9/f.java j9/n.java
00163	Create new Socket and connecting to it	socket	j9/f.java j9/n.java
00078	Get the network operator name	collection telephony	com/amplifyframework/pinpoint/core/data/AndroidDeviceDetails.java com/appsflyer/internal/AFh1cSDK.java j4/C0440d.java j4/C1845d.java
00009	Put data in cursor to JSON object	file	com/amazonaws/mobileconnectors/s3/transferutility/TransferUtility.java o4/C0509c.java o4/C2102c.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://ovia-fertility.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/205732093485/namespaces/firebase:fetch?key=AIzaSyBtYcqe2dMjvp90jqcA65ND6EwvSgtsVX4 is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'block_unsecured_device': 'true', 'coaching_closing_time': '21:00', 'coaching_opening_time': '09:00', 'data_disclosure_confirmation_alert_text': "Within 48 hours, you will receive an email to access your report at %%EMAIL%%.\\n\\nIf you'd like to use a different email address, please update your settings.", 'data_disclosure_confirmation_alert_title': 'Request your data collection & usage report', 'data_export_confirmation_alert_text': "Within 48 hours, you will receive an email to securely download all of your Ovia data at %%EMAIL%%.\\n\\nIf you'd like to use a different email address, please update your settings.", 'data_export_confirmation_alert_title': 'Request your data export', 'disable_facebook_sign_up': 'true', 'double_email_enabled': 'true', 'enable_app_review_prompt': 'true', 'enable_birth_control': 'true', 'enable_health_pathways': 'false', 'enable_menopause_mvp': 'true', 'enable_roadblock_manual_impressions': 'false', 'hpe_interstitial': '{"display_interval": 5,"interstitial_order": [1,2,3,4]}', 'is_new_daily_self_care_checklist': 'false', 'leaderboard_use_sdk_click_tracking': 'false', 'manual_impression_counting': 'true', 'menu_item_healthcare_info_enabled': 'true', 'ovia_care_team_image_url': 'https://assets.oviahealth.com/images/app-images/common/care_team_headshot_combined.png', 'ovia_plus_badge_enabled': 'true'}, 'state': 'UPDATE', 'templateVersion': '108'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.ACCESS_COARSE_LOCATION, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_NETWORK_STATE, android.permission.VIBRATE, android.permission.WRITE_EXTERNAL_STORAGE
Other Common Permissions	5/44	android.permission.AUTHENTICATE_ACCOUNTS, com.google.android.gms.permission.AD_ID, 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
api.oviahealth.com	ok	**IP:** 34.232.41.92 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
giveusashout.org	ok	**IP:** 104.21.32.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
survey.oviahealth.com	ok	**IP:** 52.207.137.143 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
sinapps.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
s3-us-west-1.amazonaws.com	ok	**IP:** 52.219.194.88 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
talksuicide.ca	ok	**IP:** 198.100.150.129 **Country:** Canada **Region:** Quebec **City:** Beauharnois **Latitude:** 45.316780 **Longitude:** -73.865898 **View:** Google Map
www.babylist.com	ok	**IP:** 104.18.17.11 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
play.google.com	ok	**IP:** 142.250.179.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
twitter.com	ok	**IP:** 162.159.140.229 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 142.250.74.68 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sgcdsdk.s	ok	No Geolocation information available.
user.oviahealth.com	ok	**IP:** 3.217.83.139 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

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
oviahealth.com	ok	**IP:** 52.20.8.175 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
sattr.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
d2sz0eblmkz2aa.cloudfront.net	ok	**IP:** 18.155.173.109 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sars.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
988lifeline.org	ok	**IP:** 172.67.74.176 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sregister.s	ok	No Geolocation information available.
pinpoint.us-gov-west-1.amazonaws.com	ok	**IP:** 56.136.222.135 **Country:** United States of America **Region:** North Carolina **City:** Raleigh **Latitude:** 35.842781 **Longitude:** -78.633690 **View:** Google Map
scdn-ssettings.s	ok	No Geolocation information available.
www.example.com	ok	**IP:** 23.220.73.43 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map
ovia-fertility.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.instagram.com	ok	**IP:** 31.13.70.174 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
www.labcorp.com	ok	**IP:** 104.18.31.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
securepubads.g.doubleclick.net	ok	**IP:** 142.250.74.66 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.ngs.ac.uk	ok	**IP:** 130.246.140.235 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Appleton **Latitude:** 51.709511 **Longitude:** -1.361360 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.saptel.org.mx	ok	**IP:** 172.67.133.117 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
scdn-stestsettings.s	ok	No Geolocation information available.
www.pieta.ie	ok	**IP:** 18.238.96.22 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.lifeline.org.au	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
instagram.com	ok	**IP:** 31.13.70.174 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.crisistextline.org	ok	**IP:** 35.243.138.147 **Country:** United States of America **Region:** South Carolina **City:** North Charleston **Latitude:** 32.888561 **Longitude:** -80.007507 **View:** Google Map
findahelpline.com	ok	**IP:** 172.67.132.66 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
apm.oviahealth.com	ok	**IP:** 54.172.1.72 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
slaunches.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
s3.amazonaws.com	ok	**IP:** 52.217.113.16 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.spuk.org.uk	ok	**IP:** 35.214.115.6 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
sapp.s	ok	No Geolocation information available.
www.pinterest.com	ok	**IP:** 151.101.128.84 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
connect.oviahealth.com	ok	**IP:** 3.217.83.139 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.amplify.aws	ok	**IP:** 13.224.53.49 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
sviap.s	ok	No Geolocation information available.
oviahealth.onelink.me	ok	**IP:** 18.155.173.39 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
d2duuy9yo5pldo.cloudfront.net	ok	**IP:** 18.238.96.29 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.oviahealth.com	ok	**IP:** 52.20.8.175 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sts.amazonaws.com	ok	**IP:** 209.54.177.164 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
acs.amazonaws.com	ok	No Geolocation information available.
text50808.ie	ok	**IP:** 104.21.16.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
pinpoint.us-west-2.amazonaws.com	ok	**IP:** 18.238.96.98 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
webchat.helpshift.com	ok	**IP:** 18.155.173.65 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
pinpoint.us-east-1.amazonaws.com	ok	**IP:** 18.155.173.12 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
svalidate.s	ok	No Geolocation information available.
www.amazon.com	ok	**IP:** 18.238.90.46 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.enfamil.com	ok	**IP:** 18.238.96.84 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
events.oviahealth.com	ok	**IP:** 34.198.52.249 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

EMAILS

EMAIL	FILE
b80d107d9c22782e1ef6@apm.oviahealth	f6/AbstractC0388a.java
b80d107d9c22782e1ef6@apm.oviahealth	f6/AbstractC1604a.java
bugs@helpshift.com	com/helpshift/activities/HSDebugActivity.java
no-reply@accounts.oviahealth support@oviahealth.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Amazon Mobile Analytics (Amplify)	Analytics	https://reports.exodus-privacy.eu.org/trackers/423
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Apptentive	Analytics	https://reports.exodus-privacy.eu.org/trackers/115
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
HelpShift		https://reports.exodus-privacy.eu.org/trackers/58
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

HARDCODED SECRETS

POSSIBLE SECRETS
"appsflyer_dev_key" : "bokoN4m7ZJ3cz4tihzXstc"
"password" : "Contraseña"
"google_crash_reporting_api_key" : "AIzaSyBtYcqe2dMjvp90jqcA65ND6EwvSgtsVX4"
"file_provider_authority_suffix" : ".fileprovider"
"google_api_key" : "AIzaSyBtYcqe2dMjvp90jqcA65ND6EwvSgtsVX4"
"password" : "Password"
"firebase_database_url" : "https://ovia-fertility.firebaseio.com"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFFFFFFFFFFFFFF
gL88T2vBvJS+jBemUvhPpVS5IeaU7cU4wFVgyT6PJl7pFldWXOd3mZxVZlQUSll5
NOrE2caDXO4nkFR2Fjy7NgGPKtPlIg1WAorknI/US68=
vpqgk7W2OO4+emKKnTSxckIsP1c64LGVSWcdsnDvr3w=
9rXsTdb/WXYONX554dN5CJ2eqpcy9gFPMPi8uAjaHTA=
1VeJuVnEfsh9S8+TnOEDCfIzscTATtniwvJaQ7/W6I8=
aC7c3pDenGsdb0eFildzKOBrhobw8fKkmd52rTlBEKM=

POSSIBLE SECRETS
o5W1eROpLyVNcsDGW3Y0lGc2x/V+mDPvMXouv3gbW6M=
joxZSCFIfSio2J1Z0g3HMtlcDGNvogfMyrj1e2b+qPNv6DXnDVXfwkgCXW9zFWFC
qUEdP6yfmpdCkPVqoE8EyrX/MPjGh4YKRo5g3kOeMoc=
da0edfb95610f25ad4e5abcc210c14c8
hhtrMjcGMTQSGdrv1+l2gakNTe0Pfchc8VT5kRHtsehlafuJ8JEE4iewNV4y5I/U
RSyr2AK130nKbepDTsaNV0Uv17TWUb4O6ebIiV3GgVs=
nIX5dAPvXYWFIvHlyxyLt0TnZ91UnAjFxZwf2qcoWSGcs+p5B5p88VCOzepPfMpE
zahwJ4oRFMB+Gn9BGkfZDZ8TzDEfKTB8Y6I4bT4vlwkVFXvqlnkWd7htbiUzWQyR
AZwRbSS9Tjg/vY6NNyDfd3mU35mZBbQduzRpliDRt3qUNjlKylmreq0JkiCiO6dF
url64=aHR0cHM6Ly9zdXJ2ZXkub3ZpYWhlYWx0aC5jb20vdHlwZS9waHE5L2ludHJv
1eWk7vHD3Ee+FybzKEoWLH07Pvdxo5flYR768ntLvpJZNSFjE7xgNzi+al9tiZC4
C6OPKdOx6rUdfDdOmaUimt8yM1FrOv7bKCITdJ0Uo74WwXDfvXouJ4oz4kHBjTSk
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
20140304181021141-2ebd3e9cc6be854
w1mRpvC09hSNbQ10UvFXagm2P4TWR/T2KztJ+buPFQZnRnjxpdFVScAm9trUP6jM
5181942b9ebc31ce68dacb56c16fd79f

POSSIBLE SECRETS
XCj6cS5OVeEeObzd394PGDbjTuQh+vSye2UT6221ugsKtO2/oznWOSes2cnebrVR
MbAcGuLi+XGl3MsgqAiQYLikemL120ZFxn+dIhaD+rHWJuTeO/M8+1c58cczHjCs
k8GEQUoJxJPI/0jAlfeUix8QD7WaaXAfMcSQAzrpgrU=
Cv/m6MvBjdOit7tT7cC+xPCpFEqovwYj4XIOcXUxCMs=
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
hwvIMOeohSBrCWT4pVkQok22g/l0cZbbqOTmNbjObWwcwhLlaFMNibQmd2cIB1Vb
SfaCE2ReDSQ3+KDKcvA6SSrX7nuWYsM/FN3ZFmlH0dA=
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
515d6767-01b7-49e5-8273-c8d11b0f331d
I5l5b06e/m6OPcJVryww5aceHDWuWNMRDm4mYVrBvJQ=
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
z3i9M2k4RJ/f7GArNBcGbUcpUFpuRmLev6S20UO7Vqs=
A3EfeXObjqx38Tdc4wdTZSQNpfpw6YVck+944M4A/m0=
ae2044fb577e65ee8bb576ca48a2f06e
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
bObXLZFRWAdU6+me08AeNX2ciqxi45ddv3QSqAplzos=
c9c45690afdef93a58618d04b99d01f0

POSSIBLE SECRETS
MIrDuKB7N0O22daoYjLtFOJg5TtVRHK1+0ktwmGNtdU=
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
s7rU1m4XsqJ83s2reIjdkboWJYkg+gYouDrDcn3Ghpw=
cZ2qwY2ZIJRch325gepGJtH7dQ9IcqmfWvaHdfiFi6Y=
JLulXGPEHVwHK+0FG96HP9my+NvwpTQbwIaIZrjn9OU=
nVNp1WYfnkUt4CgZM9ftj8WNocg8ldySiFlqCJaJia4=
Cv0JAL9ptzpRvgIi9AFTFGn0l5MhpPgpRN4VfZybymKMuiqBn9AG0bgJaX/QotAk
b4378d52cd6991e642c1503aa54555d0
xLOAO7msIR4UFUyldUn5stL2wwbLdISu2CSlTLg4f6Q=
RKC3mFMqGi7xOgQ7s39JMoZe9bnzGCFipcdUUf0vlgHDkBg7SvMkVmBGpwLs06ia
uJ6tafbdnitpIiJcEDt3zh4lzBZEYeFsW45S60suhbKyZNy2K2MuNEbuksualim4
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
url64=aHR0cHM6Ly9zdXJ2ZXkub3ZpYWhlYWx0aC5jb20vdHlwZS9lcGRzL2ludHJv
BkxOKZDOMH8NUFJEmpCq1X+PtIP0kLI1Ua0ujwsrkUE=
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
3LpdW89cIASEFv5WvS5ZDEWsiVGQitP33SL3WZgJ6zE=

POSSIBLE SECRETS
fxU2A2MjpZ4aJWGzXeMNURilSCaKosw3oXImrqnhSVmXB+tMi32JakdNlHCV3t0c
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
1tXSieficgPhud4YihA+CzunTlb+yA05iyb1BkAzMoc=
hMVcCX1S6+m7rVEDNdCHhVgXRFILMOQ9RgLSmTdPHeNgAU8CbmBsymKBuqLQcQaU
iibTgWRTbrwM2W7HZGJP5cjM0DLiCyA9TVVy1genRaa4nvgE3+CiRN/Fx87DVDsO
iJiFXDBrMwFOGpG8WmWNKc3sGwXbWv8N6fPQac0mMm0=
lsjUo68NMWNsPUz4dBIEYtWAZHRXaEljQLBgt48XQs4=
eeEXrpj8nQwF2yBkORcRAd0iFVkdVdb2kizLxXIL
Q+fOnDUQnIPH75lusFutOgWOI4DeJ6z7X13oo1pZ5m19Kfyi56UOJglWSBqO3AzA
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
sK9i540XcONymgaiZVMKYXr1VbNcwMhjwo2LFhhSCFg=
6vt+8E5GP5AwoxquDM0Y7lVJzS23/VCjNo5D8xB8rgAaaF6IhToGZhlIAUkgigHl
1ZhioNexfONxLbr8oNixHPTbX/qv3RsJiyYoeeb0m+g=
8UC+BMIoCN+KAKrN9TZmuJsGMmo3RUHS+FjVMSp9QfgjxjGZ10kqO/oSdOn5Rw29
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
1OxyLDHu2cwu0U7XKtDO3q+DghLeQ8xcTgpGCDWDuEeCcfs+HPxSt8kldIfiq1K0
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed

POSSIBLE SECRETS
tVSI3GZQAGRITfe/VNiB0JAqJe5Pfq0lPruET3IJQ2F3N6dl8hPg+ZOAK3nXD45u
Ee4p/yPQz67p3LoSNbpt1G8K9rDuoWxBYT8E4CbWyr8=
1yJaDnXEM3em29nHb3kYjIOvpW6Mkce5Fji3syGd7T0=
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
gzR6fJL0MpYPfJ/UkFL9UHjS7jlytQ+eyVRsQJTsxzK4yqDaskM4UtldyBDUp+Z9
r0MNv9zqwvoUwASL1pBJjOA1OkDa8Kcs5NaA6VOkJEI=
Y0trGqGVEUAa7A3LYgSQFKe4N9h1BuTC7OKFYCHfLSg=
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
5BhEc19mhLCb3gixLpO/usqpdcrz8iDHUvKRNr8tUAX9rUzF0wog6vEOJrftvcpW
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
6CWPidOWJZFxRWI8V7yi3OiMbOhIWZX/jTayTGRwqCM0W8dtKHQOPe60TuQicfhG
3PwoDnm3HnsskB+3ZnJHoZ7BzV0InxUqaAwJBlSwKFs=
ZHFOx+FjaOsul7gEkIcfA8auDnyRWXmT0qbiHVEO6U1RLulNSOFK3tPEgm+pvQxr
Eg2eC3eNesWzbAUINzxj1mXRcYgmzS654CxZFoVQbAM=
8Xr1ilYJHo+oWZQAYAG91DIHBuqEmXK8yHtxL6KkyfU=
zmLnsak1Fo/LHy30EeWswBCxcOoFKuH08l3DkSTUgzb476o6nI+C8ZUC+d8tLJwZ

POSSIBLE SECRETS
y+BEEb1lYOUGwTehZ9VIg/2gibmtEOjDZzKXHhs5BV0=
sjYkfzJTuYKxh1jvZaP9n5dx9JGmzJotOUC/vdvgi4M=
9722a817fe03426f6858ebf333b15fb6
uxIInGM9FQ+1gujg5A7z9lJxIqStl6tvqqzSbuEi494=
Ls+ZUCEdSGy+47NpfWc5WNy2WCTB2lhysvWY8PCvkdyqiw8HkO3XVSxwPIsY4tvv
r6m9xWOlfK6iHuNH3QiJQf71aQCKDM6NhABQId+yaKg=
s16u0iwtqlokf4v9cpgne8a2amdrxz735hjby
X9PgbTHLX0FFxbl3gdPDuVwcglfXy5CDrzo8siaVNaH+OIJ6JI34Wu3QK5rLega4
9mv9Ihk+HlE8P3WJWSjhrxWrdB7cEu1gaxdteA5kBJ6DKumpWYk1Q5Vf8aocVg4i
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
Jz2tk/JKeGJKcc4wwXH5Pf6ZM64fYgV4wWxByPOgNQE=
s1ejGoWFNJedDDJqGqL3B22F5ZMvy0oaymBcWJepS9Hv4/6KtsHBpmbtFfwgqqen
HeBkX9XaSpC6sV82I6X2HUgm82vH8VhIWt26LGkrI3A=
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
B1472D2B7A71B2988B1084F9CF3C31BB
7qOZVP58PfP3kLkbSBo98onihlohkIEpZC40FvE5nnCJ8ryn0NERK9JAnlww55zq
tfuuP59pzWN+H8zv1geT3jADiBKBGMQRjmCPoIvL5f45Lvl5qgJ0PgBqZF4WPnQj

POSSIBLE SECRETS
sdX902x/AS9226TxUXaqji9wP1uHqRQA8nkg2YMN1TcruTTaw008l9z5V3jZGjLO
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e696131163014060355040713 0d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e060355040313 07416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43 616c69666f726e6961131630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307 416e64726f69643110300e060355040313 07416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b30090603550406130255533113301106035504081 30a43616c69666f726e6961131630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d01010405000382010100 6dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
XFxH1z0dBuMDP7aWA+P/3WKwW9qr8sC2ASjEfciaKHfSLryjCNl4cmJgfsh2Tylb
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
SMfJnKfhfLLyTw7dzHC+3CXVRNFLWK4N2mQHKB3gm/o=
4fe433b787cd0c6927627230e2a04a3e
B3EEABB8EE11C2BE770B684D95219ECB
3X6BpH4xN6YrlQHEhlhdPIzjhXpe5RPJk1JdWWJY
tPxcLkiesd8JzrYIyuRbLGxWAQfsX+C1jrJaS2rsRu6lU/ve1b9hEzSSzo6VwqXx
gYPijpNio6OwLgbzbH6IuWSNtvp7bCV5UMbKZJCVNdg=
ysEnh8zkgcN8WwINs5FP7vGybZW2TtVSX36HO6emvdUrcCkVbC9hrF5Pe5ZSZx3i

POSSIBLE SECRETS
ZVHCdOeJUA1S4bCrFb9VMsUCP8Sf65wDnbBE+q4M36k=
ttuIHg/yfWDxJlotLoMLf9WBnVTbWFFKY03C8KHR8FAhIQHccw4LaDLJatYkpo23
7633365a4292b80d107d9c22782e1ef6
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d01010405003081943 10b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e0603550403130 7416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d 301e170d303830343135323333635365a170d333530393031323333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e2056696577311030 0e060355040b1307416e64726f69643110300e0603550403130 7416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d 30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e0603550403130 7416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d01010405000382010100 19d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
w5tjCRfZfXWJzckDvIkXwf5aGJEVejLzfxhnwyqJH5E=
24f7+wNdQe8HQwz0gPH2QIzxUp8iQNA20yBU7Dg74Sc=
beFEMZ/YBSUug4MSXb2BKymKiM6ZxOOlxExWa37jMlM=
3-d861b25a-1edf-11eb-adc1-0242ac120002
KHu8Xbxzr2mu9S25CNgKE5zXBf18Zj2waiAPYoFRjyhOXCyg+mYLv2x/JjCH7GjX
xcWDoPM3ZfO4P10VSUmZKRTMvsXPXnglJL31bwAJBgJGdSUy2IQG17s4MILOncV2
CkzLLxV5zSb+jeaEDnt9Q3eBrpVMtqnw6wBKNocN2YzoApdHEqHkRi4x0VOMDtd4

POSSIBLE SECRETS
mkunJHFc5vhTAVOcsaNSYx7OvFB6slgbORGrA/joIDO0IYq5rQvDcAbp2AI6CPUh

PLAYSTORE INFORMATION

Title: Ovia Cycle & Pregnancy Tracker

Score: 4.498754 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.ovuline.fertility

Developer Details: Ovia Health, Ovia+Health, None, https://www.oviahealth.com, support@oviahealth.com,

Release Date: Jan 14, 2015 **Privacy Policy:** Privacy link

Description:

At Ovia Health by Labcorp, we're here to empower women with personalized tools and data-driven insights that support every stage of their health journey—helping them make informed decisions and get the care they need. Whether you're tracking your period, trying to get pregnant, monitoring your pregnancy, or tracking your health, join the millions of Ovia users. Voted one of the best pregnancy and fertility tracker apps, Ovia helps you stay on top of all your women's health needs—tracking your pregnancy, menstrual cycle , period and ovulation predictions, postpartum recovery, perimenopause symptoms, menopause support, and overall wellness, all in one place! YOUR HEALTH IN YOUR HANDS ◆ Personalized email summaries and reminders to help you make the most of your experience and manage your health ◆ Period & Fertility calendar - Fertility forecasting algorithm predicts your fertility widows and ovulation cycles. ◆ Pregnancy - Baby growth calendar, due date countdown, bump and fetal movement tracker, and more. Watch your baby grow, track your symptoms, and learn what to expect each week. ◆ Postpartum Experience - personalized recovery modes based on delivery (vaginal, c-section, VBAC), symptom tracking, and more. ◆ Perimenopause & Menopause support - comprehensive health tracking for real-time alerts & personalized feedback. ◆ Access over 2,000 free expert articles on fertility, ovulation, conception, postpartum, menopause & reproductive health. OVULATION CALCULATOR & FERTILITY TRACKER ◆ Fertile window and ovulation time predictions and a daily fertility score. An ovulation app that helps you know when you're ovulating when trying to conceive (TTC). PERIOD AND MENSTRUAL CYCLE TRACKER ◆ A period tracker with customizable data logging inclusive of symptoms, moods, sex, and nutrition. ◆ Support for regular & irregular menstrual cycles. ◆ Birth control tracking PREGNANCY & POSTPARTUM ◆ A personalized, 12-month program focused on birth recovery, postpartum conditions and complications, reproductive planning, return to work support, mental health, & more. PERIMENOPAUSE & MENOPAUSE SUPPORT ◆ Symptom tracking, education, and support to navigate perimenopause & menopause confidently. STAY UP TO DATE ON YOUR PREGNANCY WITH ESSENTIALS ◆ Pregnancy Week by Week: Know what to expect each week with a baby due date countdown and weekly videos and content about pregnancy symptoms, body changes, & baby tips. ◆ Pregnancy Tracker and Baby Growth Calendar: Compare your baby's weekly size to a fruit, toy, pastry item, or animal. View 3D illustrations of your baby each week & track baby's growth. ◆ My Baby Names: Swipe through thousands of baby names. Save your favorites. ◆ Baby Hand and Foot Size: See a life-size image of how big your baby's hands and feet are today compared to how big they'll be at your due date! ◆ Bump Tracker: Keep a record of your growing baby bump in countdown. ◆ Safety Lookup Tools: Use lookup tools for symptoms & food safety. ◆ Kick Counter & Contraction Timer: Count baby kicks & contractions as your due date approaches. OTHER FEATURES OUR MEMBERS LOVE ◆ Friends & Family Sharing: Add your spouse, partner, sibling, or your BFF to share your daily updates. ◆ Privacy and Security: Add an extra layer of protection by adding a PIN to your account. ◆ Apple Health & Fitbit Integrations: Share data from Ovia to the Apple Health app. Sync your Fitbit to share steps, sleep & weight with Ovia. OVIA HEALTH BY LABCORP Ovia Health by Labcorp is the leading digital health companion for women across their entire health journey, from general and preventive health through perimenopause and menopause. Have Ovia Health by Labcorp through your employer or health plan? Download the app, enter your plan info, and access premium tools like health coaching, personalized content, and programs for birth control tracking, endometriosis, PCOS, & more. CUSTOMER SERVICE We're always working to improve your experience. Email us: support@oviahealth.com

SCAN LOGS

Timestamp	Event	Error
2025-09-01 06:57:00	Generating Hashes	OK
2025-09-01 06:57:00	Extracting APK	OK
2025-09-01 06:57:00	Unzipping	OK
2025-09-01 06:57:01	Parsing APK with androguard	OK
2025-09-01 06:57:01	Extracting APK features using aapt/aapt2	OK
2025-09-01 06:57:01	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 06:57:04	Parsing AndroidManifest.xml	OK
2025-09-01 06:57:04	Extracting Manifest Data	OK
2025-09-01 06:57:04	Manifest Analysis Started	OK
2025-09-01 06:57:05	Performing Static Analysis on: Ovia (com.ovuline.fertility)	OK
2025-09-01 06:57:05	Fetching Details from Play Store: com.ovuline.fertility	OK

2025-09-01 06:57:06	Checking for Malware Permissions	OK
2025-09-01 06:57:06	Fetching icon path	OK
2025-09-01 06:57:06	Library Binary Analysis Started	OK
2025-09-01 06:57:06	Analyzing lib/arm64-v8a/libandroidx.graphics.path.so	OK
2025-09-01 06:57:06	Analyzing lib/arm64-v8a/libtoolChecker.so	OK
2025-09-01 06:57:06	Analyzing lib/arm64-v8a/libsentry-android.so	OK
2025-09-01 06:57:06	Analyzing lib/arm64-v8a/libsentry.so	OK
2025-09-01 06:57:06	Analyzing lib/x86_64/libandroidx.graphics.path.so	OK
2025-09-01 06:57:06	Analyzing lib/x86_64/libtoolChecker.so	OK
2025-09-01 06:57:06	Analyzing lib/x86_64/libsentry-android.so	OK
2025-09-01 06:57:06	Analyzing lib/x86_64/libsentry.so	OK
2025-09-01 06:57:06	Analyzing lib/armeabi-v7a/libandroidx.graphics.path.so	OK

2025-09-01 06:57:06	Analyzing lib/armeabi-v7a/libtoolChecker.so	OK
2025-09-01 06:57:06	Analyzing lib/armeabi-v7a/libsentry-android.so	OK
2025-09-01 06:57:06	Analyzing lib/armeabi-v7a/libsentry.so	OK
2025-09-01 06:57:06	Analyzing lib/x86/libandroidx.graphics.path.so	OK
2025-09-01 06:57:06	Analyzing lib/x86/libtoolChecker.so	OK
2025-09-01 06:57:06	Analyzing lib/x86/libsentry-android.so	OK
2025-09-01 06:57:06	Analyzing lib/x86/libsentry.so	OK
2025-09-01 06:57:06	Analyzing apktool_out/lib/arm64-v8a/libandroidx.graphics.path.so	OK
2025-09-01 06:57:06	Analyzing apktool_out/lib/arm64-v8a/libtoolChecker.so	OK
2025-09-01 06:57:06	Analyzing apktool_out/lib/arm64-v8a/libsentry-android.so	OK
2025-09-01 06:57:06	Analyzing apktool_out/lib/arm64-v8a/libsentry.so	OK
2025-09-01 06:57:06	Analyzing apktool_out/lib/x86_64/libandroidx.graphics.path.so	OK

2025-09-01 06:57:06	Analyzing apktool_out/lib/x86_64/libtoolChecker.so	OK
2025-09-01 06:57:06	Analyzing apktool_out/lib/x86_64/libsentry-android.so	OK
2025-09-01 06:57:06	Analyzing apktool_out/lib/x86_64/libsentry.so	OK
2025-09-01 06:57:06	Analyzing apktool_out/lib/armeabi-v7a/libandroidx.graphics.path.so	OK
2025-09-01 06:57:06	Analyzing apktool_out/lib/armeabi-v7a/libtoolChecker.so	OK
2025-09-01 06:57:06	Analyzing apktool_out/lib/armeabi-v7a/libsentry-android.so	OK
2025-09-01 06:57:06	Analyzing apktool_out/lib/armeabi-v7a/libsentry.so	OK
2025-09-01 06:57:06	Analyzing apktool_out/lib/x86/libandroidx.graphics.path.so	OK
2025-09-01 06:57:06	Analyzing apktool_out/lib/x86/libtoolChecker.so	OK
2025-09-01 06:57:06	Analyzing apktool_out/lib/x86/libsentry-android.so	OK
2025-09-01 06:57:06	Analyzing apktool_out/lib/x86/libsentry.so	OK
2025-09-01 06:57:06	Reading Code Signing Certificate	OK

2025-09-01 06:57:06	Running APKiD 2.1.5	OK
2025-09-01 06:57:13	Detecting Trackers	OK
2025-09-01 06:57:19	Decompiling APK to Java with JADX	OK
2025-09-01 06:57:43	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 06:57:43	Decompiling classes2.dex with JADX	OK
2025-09-01 06:57:51	Decompiling classes4.dex with JADX	OK
2025-09-01 06:58:00	Decompiling classes.dex with JADX	OK
2025-09-01 06:58:10	Decompiling classes3.dex with JADX	OK
2025-09-01 06:58:19	Decompiling classes5.dex with JADX	OK
2025-09-01 06:58:24	Decompiling classes2.dex with JADX	OK
2025-09-01 06:58:32	Decompiling classes4.dex with JADX	OK
2025-09-01 06:58:41	Decompiling classes.dex with JADX	OK

2025-09-01 06:58:50	Decompiling classes3.dex with JADX	OK
2025-09-01 06:58:59	Decompiling classes5.dex with JADX	OK
2025-09-01 06:59:05	Converting DEX to Smali	OK
2025-09-01 06:59:05	Code Analysis Started on - java_source	OK
2025-09-01 06:59:11	Android SBOM Analysis Completed	OK
2025-09-01 06:59:23	Android SAST Completed	OK
2025-09-01 06:59:23	Android API Analysis Started	OK
2025-09-01 06:59:33	Android API Analysis Completed	OK
2025-09-01 06:59:33	Android Permission Mapping Started	OK
2025-09-01 06:59:42	Android Permission Mapping Completed	OK
2025-09-01 06:59:43	Android Behaviour Analysis Started	OK
2025-09-01 06:59:56	Android Behaviour Analysis Completed	OK

2025-09-01 06:59:56	Extracting Emails and URLs from Source Code	OK
2025-09-01 07:00:02	Email and URL Extraction Completed	OK
2025-09-01 07:00:02	Extracting String data from APK	OK
2025-09-01 07:00:02	Extracting String data from SO	OK
2025-09-01 07:00:02	Extracting String data from Code	OK
2025-09-01 07:00:02	Extracting String values and entropies from Code	OK
2025-09-01 07:00:09	Performing Malware check on extracted domains	OK
2025-09-01 07:00:22	Saving to Database	OK

Report Generated by - MobSF v4.4.0

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.