ANDROID STATIC ANALYSIS REPORT

KidControl Circles (6.0.19)

File Name:	base.apk
Package Name:	ru.kidcontrol.gpstracker
Scan Date:	Aug. 11, 2024, 12:47 p.m.

App Security Score:	42/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	ℹ INFO	✓ SECURE	HOTSPOT
5	19	2	1	2

FILE INFORMATION

File Name: base.apk
Size: 40.82MB
MD5: a3c7e4a1ed7e8779faa299758bf2d003
SHA1: f11669d4a872d770e10593a4aea98e9156d00497
SHA256: 044d5959f80b03c43276f9d43463bb685a92a77053a12e1250ce0d5bdc8f6400

APP INFORMATION

App Name: KidControl Circles
Package Name: ru.kidcontrol.gpstracker
Main Activity: ru.kidcontrol.gpstracker.MainActivity
Target SDK: 33
Min SDK: 24
Max SDK:
Android Version Name: 6.0.19
Android Version Code: 275

APP COMPONENTS

Activities: 12
Services: 24
Receivers: 18
Providers: 8
Exported Activities: 2
Exported Services: 3
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=RU, L=St.Petersburg, O=KdControl, CN=Kidcontrol dev.
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-05-20 15:36:21+00:00
Valid To: 2040-05-13 15:36:21+00:00
Issuer: C=RU, L=St.Petersburg, O=KdControl, CN=Kidcontrol dev.
Serial Number: 0x555ca9f5
Hash Algorithm: sha1
md5: 813e7cb25ad20449e42e3ef8ce4aa2e5
sha1: 8e21fc3b7da5ed0b5a5ac2ad8274d8b9c3c777c2

sha256: 6aa44035f37fb240b0fcbcf43f137e37464154181d8a3f92b3669ce92700d639
sha512: 304315747df71297105f90444bceb861f258f58087c0ea7f6347715d98843069c99f9503bbe38bb2a454649fbed82ea20e2b30ec07c8a4a784f74d4a737cec45
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: cc332fc41912cc808dcb522ba6f51864b865bf731d064c451a8222da40c23bc4
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
oppo.permission.OPPO_COMPONENT_SAFE	signature	permission specific to OPPO devices	It is used to grant apps the ability to access certain system-level features or components that are otherwise restricted for security reasons. This permission ensures that only trusted applications can interact with sensitive parts of the OPPO system.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
com.huawei.hms.permission.ACTIVITY_RECOGNITION	unknown	Unknown permission	Unknown permission from android reference
com.huawei.permission.external_app_settings.USE_COMPONENT	signature	permission specific to Huawei devices	It is used to grant apps the ability to access certain system-level features or components that are otherwise restricted for security reasons. This permission ensures that only trusted applications can interact with sensitive parts of the Huawei system.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.TAGS check
SIM operator check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</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.HARDWARE check
Build.BOARD check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
ru.kidcontrol.gpstracker.MainActivity	Schemes: https://, Hosts: kid-control.com,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

🔒 NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	kid-control.com server.chitas.mobi webcoders.ru local.emulator.com	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

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: **1** | WARNING: **9** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_configuration]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) 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.
5	Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	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.
9	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.
10	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.
11	Service (com.transistorsoft.tsbackgroundfetch.FetchJobService) 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.

CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ch/qos/logback/classic/android/LogcatAppender.java ch/qos/logback/classic/net/SimpleSocketServer.java ch/qos/logback/classic/pattern/TargetLengthBasedClassNameAbbreviator.java ch/qos/logback/classic/spi/ThrowableProxy.java ch/qos/logback/core/net/DefaultSocketConnector.java ch/qos/logback/core/net/SocketConnectorBase.java ch/qos/logback/core/subst/Node.java com/afollestad/materialdialogs/internal/c.java com/huawei/agconnect/core/c/b.java com/huawei/agconnect/core/c/c.java com/huawei/agconnect/core/c/d.java com/huawei/agconnect/core/provider/AGConnectInitializeProvider.java com/huawei/hms/activity/BridgeActivity.java com/huawei/hms/activity/ForegroundBusDelegate.java com/huawei/hms/activity/internal/ForegroundInnerHeader.java com/huawei/hms/adapter/AvailableAdapter.java com/huawei/hms/adapter/BaseAdapter.java com/huawei/hms/adapter/BinderAdapter.java com/huawei/hms/adapter/InnerBinderAdapter.java com/huawei/hms/adapter/OuterBinderAdapter.java com/huawei/hms/adapter/ui/BaseResolutionAdapter.java com/huawei/hms/adapter/ui/NotInstalledHmsAdapter.java com/huawei/hms/adapter/ui/UpdateAdapter.java com/huawei/hms/android/HwBuildEx.java com/huawei/hms/android/SystemUtils.java com/huawei/hms/api/BindingFailedResolution.java com/huawei/hms/api/FailedBinderCallBack.java com/huawei/hms/api/HuaweiApiClientImpl.java com/huawei/hms/api/HuaweiMobileServicesUtil.java com/huawei/hms/api/IPCCallback.java com/huawei/hms/api/IPCTransport.java com/huawei/hms/api/ResolutionDelegate.java com/huawei/hms/api/b.java com/huawei/hms/availableupdate/a.java com/huawei/hms/base/ui/a.java com/huawei/hms/common/HuaweiApi.java com/huawei/hms/common/api/AvailabilityException.java com/huawei/hms/common/data/DataHolder.java com/huawei/hms/common/internal/BaseHmsClient.java com/huawei/hms/common/internal/ConnectionErrorMessages.java com/huawei/hms/common/internal/DialogRedirect.java com/huawei/hms/common/internal/HmsClient.java com/huawei/hms/common/internal/RequestHeader.java com/huawei/hms/common/internal/RequestManager.java com/huawei/hms/common/internal/ResponseHeader.java com/huawei/hms/common/internal/ResponseWrap.java com/huawei/hms/common/internal/TaskApiCall.java com/huawei/hms/common/util/AGCUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/huawei/hms/common/util/Base64Utils.java com/huawei/hms/core/aidl/f.java com/huawei/hms/device/a.java com/huawei/hms/framework/common/Logger.java com/huawei/hms/stats/a.java com/huawei/hms/stats/c.java com/huawei/hms/support/api/ErrorResultImpl.java com/huawei/hms/support/api/PendingResultImpl.java com/huawei/hms/support/api/client/ResolvingResultCallbacks.java com/huawei/hms/support/api/client/ResultCallbacks.java com/huawei/hms/support/api/core/ConnectService.java com/huawei/hms/support/api/location/common/HMSLocationLog.java com/huawei/hms/support/api/location/common/LocationClientStateManager.java com/huawei/hms/support/api/location/common/LocationRequestHelper.java com/huawei/hms/support/api/location/common/PermissionUtil.java com/huawei/hms/support/api/location/common/exception/ServiceErrorCodeAdaptor.java com/huawei/hms/support/common/ActivityMgr.java com/huawei/hms/support/hianalytics/HiAnalyticsUtil.java com/huawei/hms/support/hianalytics/HiAnalyticsUtils.java com/huawei/hms/support/log/HMSDebugger.java com/huawei/hms/ui/AbstractDialog.java com/huawei/hms/update/note/AppSpoofResolution.java com/huawei/hms/update/note/DoNothingResolution.java com/huawei/hms/update/note/NotInstalledHmsResolution.java com/huawei/hms/update/ui/NotInstalledHmsDialogHelper.java com/huawei/hms/utils/FileUtil.java com/huawei/hms/utils/HMSBIInitializer.java com/huawei/hms/utils/HMSPackageManager.java com/huawei/hms/utils/IOUtils.java com/huawei/hms/utils/JsonUtil.java com/huawei/hms/utils/PackageManagerHelper.java com/huawei/hms/utils/ReadApkFileUtil.java com/huawei/hms/utils/SHA256.java com/huawei/hms/utils/UIUtil.java com/huawei/hms/utils/Util.java com/huawei/location/a.java com/huawei/location/activity/c/c.java com/huawei/location/j/a/e/h/f.java com/huawei/location/j/a/e/h/g.java com/huawei/location/j/a/e/h/i.java com/huawei/riemann/common/api/location/SdmLocationClient.java com/huawei/riemann/gnsslocation/api/vdr/VdrLocationClient.java com/huawei/riemann/location/a.java com/huawei/secure/android/common/util/SafeBase64.java com/huawei/secure/android/common/util/SafeString.java com/intentfilter/androidpermissions/f/b.java com/transistorsoft/flutter/backgroundfetch/BackgroundFetchModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/transistorsoft/flutter/backgroundfetch/HeadlessTask.java com/transistorsoft/flutter/backgroundgeolocation/BackgroundGeolocationModule.java com/transistorsoft/flutter/backgroundgeolocation/HeadlessTask.java com/transistorsoft/locationmanager/BootReceiver.java com/transistorsoft/locationmanager/a/a.java com/transistorsoft/locationmanager/activity/TSLocationManagerActivity.java com/transistorsoft/locationmanager/adapter/BackgroundGeolocation.java com/transistorsoft/locationmanager/adapter/TSConfig.java com/transistorsoft/locationmanager/b/a.java com/transistorsoft/locationmanager/c/a.java com/transistorsoft/locationmanager/config/TSAuthorization.java com/transistorsoft/locationmanager/config/TSBackgroundPermissionRationale.java com/transistorsoft/locationmanager/config/TSNotification.java com/transistorsoft/locationmanager/config/TransistorAuthorizationToken.java com/transistorsoft/locationmanager/d/b.java com/transistorsoft/locationmanager/data/LocationModel.java com/transistorsoft/locationmanager/data/sqlite/GeofenceDAO.java com/transistorsoft/locationmanager/data/sqlite/a.java com/transistorsoft/locationmanager/data/sqlite/b.java com/transistorsoft/locationmanager/device/DeviceInfo.java com/transistorsoft/locationmanager/device/DeviceSettings.java com/transistorsoft/locationmanager/e/a.java com/transistorsoft/locationmanager/event/ActivityChangeEvent.java com/transistorsoft/locationmanager/event/AuthorizationEvent.java com/transistorsoft/locationmanager/event/GeofenceEvent.java com/transistorsoft/locationmanager/event/GeofencesChangeEvent.java com/transistorsoft/locationmanager/event/HeartbeatEvent.java com/transistorsoft/locationmanager/event/LocationProviderChangeEvent.java com/transistorsoft/locationmanager/event/MotionChangeEvent.java com/transistorsoft/locationmanager/event/TerminateEvent.java com/transistorsoft/locationmanager/geofence/TSGeofence.java com/transistorsoft/locationmanager/geofence/TSGeofenceManager.java com/transistorsoft/locationmanager/http/HttpResponse.java com/transistorsoft/locationmanager/http/HttpService.java com/transistorsoft/locationmanager/location/SingleLocationRequest.java com/transistorsoft/locationmanager/location/TSLocation.java com/transistorsoft/locationmanager/location/TSLocationManager.java com/transistorsoft/locationmanager/location/TSWatchPositionRequest.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/transistorsoft/locationmanager/logger/TSLog.java com/transistorsoft/locationmanager/logger/TSLogReader.java com/transistorsoft/locationmanager/logger/TSSQLiteAppender.java com/transistorsoft/locationmanager/logger/a.java com/transistorsoft/locationmanager/provider/TSProviderManager.java com/transistorsoft/locationmanager/scheduler/ScheduleEvent.java com/transistorsoft/locationmanager/scheduler/TSScheduleManager.java com/transistorsoft/locationmanager/service/AbstractService.java com/transistorsoft/locationmanager/service/ActivityRecognitionService.java com/transistorsoft/locationmanager/service/BackgroundTaskService.java com/transistorsoft/locationmanager/service/ForegroundNotification.java com/transistorsoft/locationmanager/service/GeofencingService.java com/transistorsoft/locationmanager/service/LocationRequestService.java com/transistorsoft/locationmanager/service/TrackingService.java com/transistorsoft/locationmanager/util/BackgroundTaskManager.java com/transistorsoft/locationmanager/util/a.java com/transistorsoft/locationmanager/util/b.java com/transistorsoft/locationmanager/util/c.java com/transistorsoft/locationmanager/util/d.java com/transistorsoft/tsbackgroundfetch/BGTask.java com/transistorsoft/tsbackgroundfetch/BackgroundFetch.java com/transistorsoft/tsbackgroundfetch/BackgroundFetchConfig.java com/transistorsoft/tsbackgroundfetch/BootReceiver.java com/transistorsoft/tsbackgroundfetch/FetchAlarmReceiver.java com/transistorsoft/tsbackgroundfetch/FetchJobService.java com/transistorsoft/tsbackgroundfetch/LifecycleManager.java com/transistorsoft/xms/g/actions/SearchIntents.java com/transistorsoft/xms/g/common/ConnectionResult.java com/transistorsoft/xms/g/common/ErrorDialogFragment.java com/transistorsoft/xms/g/common/ExtensionApiAvailability.java com/transistorsoft/xms/g/common/ExtensionPlayServicesNotAvailableException.java com/transistorsoft/xms/g/common/ExtensionPlayServicesRepairableException.java com/transistorsoft/xms/g/common/ExtensionPlayServicesUtil.java com/transistorsoft/xms/g/common/SupportErrorDialogFragment.java com/transistorsoft/xms/g/common/UserRecoverableException.java com/transistorsoft/xms/g/common/api/ApiException.java com/transistorsoft/xms/g/common/api/AvailabilityException.ja

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	va com/transistorsoft/xms/g/common/api/BooleanResult.java com/transistorsoft/xms/g/common/api/CommonStatusCodes.java com/transistorsoft/xms/g/common/api/ExtensionApiClient.java com/transistorsoft/xms/g/common/api/OptionalPendingResult.java com/transistorsoft/xms/g/common/api/PendingResult.java com/transistorsoft/xms/g/common/api/PendingResults.java com/transistorsoft/xms/g/common/api/Releasable.java com/transistorsoft/xms/g/common/api/ResolvableApiException.java com/transistorsoft/xms/g/common/api/ResolvingResultCallbacks.java com/transistorsoft/xms/g/common/api/Response.java com/transistorsoft/xms/g/common/api/Result.java com/transistorsoft/xms/g/common/api/ResultCallback.java com/transistorsoft/xms/g/common/api/ResultCallbacks.java com/transistorsoft/xms/g/common/api/ResultTransform.java com/transistorsoft/xms/g/common/api/Scope.java com/transistorsoft/xms/g/common/api/Status.java com/transistorsoft/xms/g/common/api/TransformedResult.java com/transistorsoft/xms/g/common/api/UnsupportedApiCallException.java com/transistorsoft/xms/g/common/data/AbstractDataBuffer.java com/transistorsoft/xms/g/common/data/DataBuffer.java com/transistorsoft/xms/g/common/data/DataBufferObserver.java com/transistorsoft/xms/g/common/data/DataBufferUtils.java com/transistorsoft/xms/g/common/data/Freezable.java com/transistorsoft/xms/g/common/data/FreezableUtils.java com/transistorsoft/xms/g/common/images/Size.java com/transistorsoft/xms/g/common/images/WebImage.java com/transistorsoft/xms/g/location/ActivityRecognition.java com/transistorsoft/xms/g/location/ActivityRecognitionClient.java com/transistorsoft/xms/g/location/ActivityRecognitionResult.java com/transistorsoft/xms/g/location/ActivityTransition.java com/transistorsoft/xms/g/location/ActivityTransitionEvent.java com/transistorsoft/xms/g/location/ActivityTransitionRequest.java com/transistorsoft/xms/g/location/ActivityTransitionResult.java com/transistorsoft/xms/g/location/DetectedActivity.java com/transistorsoft/xms/g/location/FusedLocationProviderClient.java com/transistorsoft/xms/g/location/Geofence.java com/transistorsoft/xms/g/location/GeofenceStatusCodes.java com/transistorsoft/xms/g/location/GeofencingClient.java com/transistorsoft/xms/g/location/GeofencingEvent.java com/transistorsoft/xms/g/location/GeofencingRequest.java com/transistorsoft/xms/g/location/LocationAvailability.java com/transistorsoft/xms/g/location/LocationCallback.java com/transistorsoft/xms/g/location/LocationRequest.java com/transistorsoft/xms/g/location/LocationResult.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/transistorsoft/xms/g/location/LocationResult.java com/transistorsoft/xms/g/location/LocationServices.java com/transistorsoft/xms/g/location/LocationSettingsRequest.java com/transistorsoft/xms/g/location/LocationSettingsResponse.java com/transistorsoft/xms/g/location/LocationSettingsResult.java com/transistorsoft/xms/g/location/LocationSettingsStates.java com/transistorsoft/xms/g/location/LocationSettingsStatusCodes.java com/transistorsoft/xms/g/location/LocationStatusCodes.java com/transistorsoft/xms/g/location/SettingsClient.java com/transistorsoft/xms/g/security/ProviderInstaller.java com/transistorsoft/xms/g/tasks/CancellationToken.java com/transistorsoft/xms/g/tasks/CancellationTokenSource.java com/transistorsoft/xms/g/tasks/Continuation.java com/transistorsoft/xms/g/tasks/OnCanceledListener.java com/transistorsoft/xms/g/tasks/OnCompleteListener.java com/transistorsoft/xms/g/tasks/OnFailureListener.java com/transistorsoft/xms/g/tasks/OnSuccessListener.java com/transistorsoft/xms/g/tasks/SuccessContinuation.java com/transistorsoft/xms/g/tasks/Task.java com/transistorsoft/xms/g/tasks/TaskCompletionSource.java com/transistorsoft/xms/g/tasks/TaskExecutors.java com/transistorsoft/xms/g/tasks/Tasks.java com/transistorsoft/xms/g/utils/Utils.java com/transistorsoft/xms/g/utils/XObject.java com/transistorsoft/xms/g/utils/XmsLog.java defpackage/c.java e/a/n/g.java e/f/a/d.java e/f/a/m/f.java e/f/b/a/a.java e/f/b/b/j.java e/h/j/a.java e/h/j/f/e.java e/h/j/f/f.java e/h/j/f/j.java e/h/k/d.java e/h/k/f.java e/h/k/g.java e/h/k/h.java e/h/k/k.java e/h/k/l.java e/h/p/e.java e/h/p/k.java e/h/r/b.java e/h/t/a0.java e/h/t/b0.java e/h/t/d0.java e/h/t/e.java e/h/t/i0.java e/h/t/j.java e/h/t/k0/c.java e/h/t/m.java e/h/t/m0/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				e/j/b/c.java e/l/a/c.java e/l/a/b.java e/o/a/a.java e/p/a/b.java e/p/b/c.java e/q/a/a.java e/s/a/c.java e/t/a.java e/u/i0.java e/u/y.java e/v/a/a/h.java f/d/a/b.java f/d/a/c.java f/d/b/j.java f/d/b/n.java f/d/b/o.java f/d/b/p.java f/h/a/a.java f/i/b/a/i/y/a.java f/i/b/b/b0/g.java f/i/b/b/l/h.java f/i/b/b/y/d.java f/i/b/b/z/b.java f/j/a/d.java f/j/a/h/c/b.java f/j/a/h/c/e.java f/j/a/h/c/g.java f/j/a/h/c/j.java f/j/a/h/c/m.java f/j/b/a/n/g.java f/j/c/a/p1.java f/j/c/b/b.java f/j/c/b/b0.java f/j/c/b/b1.java f/j/c/b/c.java f/j/c/b/d1.java f/j/c/b/e.java f/j/c/b/e0.java f/j/c/b/f0.java f/j/c/b/f1.java f/j/c/b/g.java f/j/c/b/g0.java f/j/c/b/h.java f/j/c/b/h0.java f/j/c/b/h1.java f/j/c/b/j.java f/j/c/b/j1.java f/j/c/b/k.java f/j/c/b/k0.java f/j/c/b/l0.java f/j/c/b/l1.java f/j/c/b/n.java f/j/c/b/n0.java f/j/c/b/n1.java f/j/c/b/o.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				f/j/c/b/o0.java f/j/c/b/p.java f/j/c/b/p0.java f/j/c/b/q.java f/j/c/b/q0.java f/j/c/b/s.java f/j/c/b/t.java f/j/c/b/t0.java f/j/c/b/u.java f/j/c/b/v0.java f/j/c/b/w.java f/j/c/b/w0.java f/j/c/b/x.java f/j/c/b/x0.java f/j/c/b/y.java f/j/c/b/z.java f/j/c/b/z0.java f/j/d/a/a/a/a.java f/j/d/a/a/b/e/g.java f/j/d/a/a/d/g/a.java f/j/d/a/a/d/g/f.java f/j/e/b/a/b/b.java f/j/e/b/a/b/c.java f/m/a/a.java f/o/a/b0.java f/o/a/r.java f/o/a/z.java h/a/a/g.java h/a/a/l/e.java h/a/a/l/g.java h/a/a/o/f.java h/a/a/o/h.java h/a/a/o/i.java i/a/b.java io/flutter/plugins/a/a.java io/flutter/plugins/c/c.java io/flutter/plugins/d/e.java io/flutter/plugins/f/h.java io/flutter/plugins/firebase/crashlytics/n.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundService.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingReceiver.java io/flutter/plugins/firebase/messaging/r.java io/flutter/plugins/firebase/messaging/t.java io/flutter/plugins/firebase/messaging/y.java io/flutter/plugins/googlemaps/GoogleMapController.java io/flutter/plugins/googlemaps/f0.java io/flutter/plugins/imagepicker/b.java io/flutter/plugins/imagepicker/g.java io/flutter/plugins/urllauncher/a.java io/flutter/plugins/urllauncher/b.java io/flutter/plugins/urllauncher/c.java me/zhanghai/android/materialprogressbar/BaseProgressLayerDrawable.java me/zhanghai/android/materialprogressbar/MaterialProgressBa

NO	ISSUE	SEVERITY	STANDARDS	FILES
				me/zhanghai/android/materialprogressbar/MaterialProgressBar.java org/slf4j/helpers/Util.java
2	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	ch/qos/logback/core/net/ssl/SSLContextFactoryBean.java f/j/d/a/a/d/e.java l/g0/c.java
3	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	f/n/a/f/b/b.java
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/huawei/hms/api/HuaweiApiAvailability.java com/huawei/hms/api/HuaweiApiClientImpl.java com/huawei/hms/base/device/BuildConfig.java com/huawei/hms/common/PackageConstants.java com/huawei/hms/framework/common/BuildConfig.java com/huawei/hms/framework/common/hianalytics/HianalyticsHelper.java com/huawei/hms/framework/network/grs/BuildConfig.java com/huawei/hms/framework/network/grs/g/k/a.java com/huawei/hms/framework/network/grs/h/a.java com/huawei/hms/location/BuildConfig.java com/huawei/hms/location/base/BuildConfig.java com/huawei/hms/support/api/PendingResultImpl.java com/huawei/hms/support/hianalytics/HiAnalyticsUtil.java com/huawei/hms/support/hianalytics/a.java com/huawei/location/router/BuildConfig.java com/huawei/wisesecurity/ucs/credential/CredentialClient.java f/j/c/a/h1.java f/j/c/a/p1.java f/j/c/a/u.java f/j/d/a/a/d/g/a.java f/j/e/c/p.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	io/flutter/plugin/editing/b.java io/flutter/plugin/platform/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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	ch/qos/logback/classic/joran/action/ConfigurationAction.java ch/qos/logback/classic/sift/ContextBasedDiscriminator.java ch/qos/logback/core/CoreConstants.java ch/qos/logback/core/net/ssl/SSL.java ch/qos/logback/core/rolling/helper/DateTokenConverter.java ch/qos/logback/core/rolling/helper/IntegerTokenConverter.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/models/NotificationDetails.java com/huawei/hms/framework/common/hianalytics/HianalyticsBaseData.java com/huawei/hms/location/LocationAvailability.java com/huawei/hms/location/LocationResult.java com/huawei/hms/support/api/location/common/LocationClientStateManager.java com/huawei/hms/support/hianalytics/HiAnalyticsConstant.java com/huawei/location/lite/common/config/b.java
7	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	f/j/a/h/c/k.java f/j/d/a/a/b/a/a.java
8	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	ch/qos/logback/core/android/AndroidContextUtil.java e/h/j/a.java e/h/j/b.java io/flutter/plugins/f/g.java io/flutter/plugins/f/h.java io/flutter/plugins/share/b.java
9	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/huawei/hms/common/internal/TransactionIdCreater.java k/z/a.java k/z/b.java k/z/d/a.java
10	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	f/j/a/h/c/k.java f/j/c/a/p.java f/j/d/a/a/b/b/b.java f/n/a/f/a/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	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	ch/qos/logback/classic/android/SQLiteAppender.java com/transistorsoft/locationmanager/data/sqlite/GeofenceDAO.java com/transistorsoft/locationmanager/data/sqlite/a.java com/transistorsoft/locationmanager/data/sqlite/b.java com/transistorsoft/locationmanager/logger/TSSQLiteAppender.java e/s/a/g/a.java f/i/b/a/i/a0/j/a0.java f/i/b/a/i/a0/j/r0.java f/i/b/a/i/a0/j/t0.java f/o/a/r.java
12	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	com/huawei/location/j/a/f/m.java
13	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	e/l/a/a.java io/flutter/plugins/imagepicker/c.java o/a/a/h.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/libpbkdf2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
3	armeabi-v7a/libTransform.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
4	armeabi-v7a/libucs-credential.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memset_chk', '__memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	armeabi-v7a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
6	x86_64/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
7	x86_64/libpbkdf2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86_64/libucs-credential.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memset_chk', '__memcpy_chk']	False warning Symbols are available.
9	x86_64/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	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', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__strncpy_chk', '__memmove_chk']	False warning Symbols are available.
10	arm64-v8a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	arm64-v8a/libpbkdf2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
12	arm64-v8a/libTransform.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
13	arm64-v8a/libucs-credential.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	arm64-v8a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	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', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__strncpy_chk', '__memmove_chk']	False warning Symbols are available.
15	x86/libpbkdf2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
16	x86/libucs-credential.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memset_chk', '__memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	armeabi-v7a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
18	armeabi-v7a/libpbkdf2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
19	armeabi-v7a/libTransform.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	armeabi-v7a/libucs-credential.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memset_chk', '__memcpy_chk']	False warning Symbols are available.
21	armeabi-v7a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
22	x86_64/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	x86_64/libpbkdf2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
24	x86_64/libucs-credential.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memset_chk', '__memcpy_chk']	False warning Symbols are available.
25	x86_64/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	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', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__strncpy_chk', '__memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	arm64-v8a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
27	arm64-v8a/libpbkdf2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
28	arm64-v8a/libTransform.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	arm64-v8a/libucs-credential.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk']	False warning Symbols are available.
30	arm64-v8a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	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', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__strncpy_chk', '__memmove_chk']	False warning Symbols are available.
31	x86/libpbkdf2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	x86/libucs-credential.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memset_chk', '__memcpy_chk']	False warning Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/24	android.permission.INTERNET, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_WIFI_STATE
Other Common Permissions	10/45	android.permission.ACTIVITY_RECOGNITION, com.google.android.gms.permission.ACTIVITY_RECOGNITION, android.permission.FOREGROUND_SERVICE, android.permission.ACCESS_NOTIFICATION_POLICY, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.CHANGE_WIFI_STATE, android.permission.ACCESS_BACKGROUND_LOCATION

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 195.15.222.169 **Country:** Switzerland **Region:** Basel-Stadt **City:** Basel **Latitude:** 47.558399 **Longitude:** 7.573270 **View:** Google Map
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
flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
master-plateau-95415.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
api.cloudpayments.ru	ok	**IP:** 178.248.238.60 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.apple.com	ok	**IP:** 2.18.68.245 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
share.here.com	ok	**IP:** 13.32.110.85 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
logback.qos.ch	ok	**IP:** 195.15.222.169 **Country:** Switzerland **Region:** Basel-Stadt **City:** Basel **Latitude:** 47.558399 **Longitude:** 7.573270 **View:** Google Map
demo.cloudpayments.ru	ok	**IP:** 178.248.239.99 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
android.googlesource.com	ok	**IP:** 172.217.218.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
maps.google.com	ok	**IP:** 172.217.19.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
circles.kid-control.com	ok	No Geolocation information available.
example.com	ok	**IP:** 93.184.215.14 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
commons.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
api.country.is	ok	**IP:** 104.26.0.226 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.251.39.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
xml.org	ok	**IP:** 104.239.240.11 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
maps.apple.com	ok	**IP:** 2.23.154.136 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
kid-control.com	ok	**IP:** 212.193.59.240 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.180.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://master-plateau-95415.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
_assertionerror@0150898._create authenticationscheme@13463476.fromstring _tileoverlayupdates@1554141099.from help@kid-control.com l_invocationmirror@0150898._withtype k_colorfilter@16065589.lineartosr _socket@14069316._readpipe _list@0150898._ofgrowabl i_rawsocket@14069316._writepipe g_builtlistmultimap@184051080.withsafema _growablelist@0150898._literal5 _datumpoint@297171995.from 7u_growablelist@0150898._literal7 _future@4048458.immediatee _colorfilter@16065589.mode tak@kid-control.com _receiveportimpl@1026248.fromrawrec eo_bytebuffer@7027147._new bb_growablelist@0150898._ofgrowabl _tileoverlayupdates@1548063751.from _casterror@0150898._create _growablelist@0150898._literal privacy@kid-control.com _growablelist@0150898._ofarray l_builtset@186144396.from w_builtlist@183235305.from v_file@14069316.fromrawpat _directory@14069316.fromrawpat c_growablelist@0150898.withcapaci storationinformation@1230124995.fromserial q_imagefilter@16065589.blur lectiontoolbarbutton@956113492.text g_bigintimpl@0150898.from n_typeerror@0150898._create _list@0150898._ofother +@hext.dart x5r_builtsetmultimap@187270276.withsafema	lib/armeabi-v7a/libapp.so

EMAIL	FILE
ngstreamsubscription@4048458.zoned _future@4048458.immediate _uri@0150898.directory lectiontoolbarbutton@835392285.text l_builtlistmultimap@184051080.copy z_timer@1026248.periodic _growablelist@0150898._literal6 _rawsocket@14069316._readpipe _list@0150898._ofefficie _httpparser@13463476.responsepa u_growablelist@0150898._ofother _builtmap@185085274.copyandche _growablelist@0150898._literal4 __datumpoint@321313943.from -_list@0150898._ofarray j_filestream@14069316.forstdin qd_growablelist@0150898._literal8 _list@0150898.empty _growablelist@0150898._literal1 _uri@0150898.notsimple gh_growablelist@0150898.generate _cookie@13463476.fromsetcoo m_growablelist@0150898._literal2 _double@0150898.fromintege x_growablelist@0150898.of _colorfilter@16065589.srgbtoline _future@4048458.zonevalue __growablelist@0150898._ofefficie _list@0150898.of 4_uri@0150898.file _list@0150898.generate _timer@1026248._internal av_nativesocket@14069316.normal _link@14069316.fromrawpat _nativesocket@14069316.pipe _growablelist@0150898._literal3	
appro@openssl.org	lib/arm64-v8a/libflutter.so
_assertionerror@0150898._create authenticationscheme@13463476.fromstring _tileoverlayupdates@1554141099.from help@kid-control.com l_invocationmirror@0150898._withtype k_colorfilter@16065589.lineartosr _socket@14069316._readpipe _list@0150898._ofgrowabl i_rawsocket@14069316._writepipe g_builtlistmultimap@184051080.withsafema _growablelist@0150898._literal5 _datumpoint@297171995.from 7u_growablelist@0150898._literal7 _future@4048458.immediatee _colorfilter@16065589.mode tak@kid-control.com	

EMAIL	FILE
talk@kid-control.com _receiveportimpl@1026248.fromrawrec eo_bytebuffer@7027147._new bb_growablelist@0150898._ofgrowabl _tileoverlayupdates@1548063751.from _casterror@0150898._create _growablelist@0150898._literal privacy@kid-control.com _growablelist@0150898._ofarray l_builtset@186144396.from w_builtlist@183235305.from v_file@14069316.fromrawpat _directory@14069316.fromrawpat c_growablelist@0150898.withcapaci storationinformation@1230124995.fromserial q_imagefilter@16065589.blur lectiontoolbarbutton@956113492.text g_bigintimpl@0150898.from n_typeerror@0150898._create _list@0150898._ofother +@hext.dart x5r_builtsetmultimap@187270276.withsafema ngstreamsubscription@4048458.zoned ._future@4048458.immediate _uri@0150898.directory lectiontoolbarbutton@835392285.text l_builtlistmultimap@184051080.copy z_timer@1026248.periodic _growablelist@0150898._literal6 _rawsocket@14069316._readpipe _list@0150898._ofefficie _httpparser@13463476.responsepa u_growablelist@0150898._ofother _builtmap@185085274.copyandche _growablelist@0150898._literal4 __datumpoint@321313943.from -_list@0150898._ofarray j_filestream@14069316.forstdin qd_growablelist@0150898._literal8 _list@0150898.empty _growablelist@0150898._literal1 _uri@0150898.notsimple gh_growablelist@0150898.generate _cookie@13463476.fromsetcoo m_growablelist@0150898._literal2 _double@0150898.fromintege x_growablelist@0150898.of _colorfilter@16065589.srgbtoline _future@4048458.zonevalue __growablelist@0150898._ofefficie _list@0150898.of 4_uri@0150898.file _list@0150898.generate _timer@1026248._internal av_nativesocket@14069316.normal _link@14069316.fromrawpat	apktool_out/lib/armeabi-v7a/libapp.so

_nativesocket@14069316.pipe
_growablelist@0150898._literal3

EMAIL	FILE
appro@openssl.org	apktool_out/lib/arm64-v8a/libflutter.so

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333

HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyBVNlkOKLZKknaZrHO6kbw3Z2kcpPSzPMk"
"file_provider_authority" : "com.transistorsoft.tslocationmanager.fileprovider"
"google_crash_reporting_api_key" : "AIzaSyBVNlkOKLZKknaZrHO6kbw3Z2kcpPSzPMk"
"firebase_database_url" : "https://master-plateau-95415.firebaseio.com"
115792089210356248762697446949407573530086143415290314195533631308867097853951
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
30820122300d06092a864886f70d01010105000382010f003082010a0282010100a3d269348ac59923f65e8111c337605e29a1d1bc54fa96c1445050dd14d8d63b10f9f0230bb87ef348183660bedcabfdec045e235ed96935799fcdb4af5c97717ff3b0954eaf1b723225b3a00f81cbd67ce6dc5a4c07f7741ad3bf1913a480c6e267ab1740f409edd2dc33c8b718a8e30e56d9a93f321723c1d0c9ea62115f996812ceef186954595e39a19b74245542c407f7dddb1d12e6eedcfc0bd7cd945ef7255ad0fc9e796258e0fb5e52a23013d15033a32b4071b65f3f924ae5c5761e22327b4d2ae60f4158a5eb15565ba079de29b81540f5fbb3be101a95357f367fc661d797074ff3826950029c52223e4594673a24a334cae62d63b838ba3df9770203010001
lEEnhl5euaIfSg9vXz1JH43pBH/xGM9fvSrfPaUZwEI=
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE

POSSIBLE SECRETS
XexrqxQZ83Dsows1I9oUUMC34QJd/x5AyWUFr5Va7Yc=
oU8dxPYnryKlPd91mK89Z7Qor1PaeT+LMYSHnhThZ+4=
470fa2b4ae81cd56ecbcda9735803434cec591fa
f8d927750a0952ffb5bd87dfb83d781ae65f7bed043a7886d1d3cdcfc94bb77a
hUIXYyX7voAFfmX9K6Tyj7UNRMoApsO3NHhichzgf1HY6Km4YpCnpT8GA4sfwulx
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
xd283h5qAcacM5zVZnbCaCYEYmyBvCzSWmcoDFc838gJ/DBCdoedE0EgOC5ZJs5s
Zsy6wzxKzkvuI5Zg91hlK7lftgUdlMXbkLzI72tnQVNXNUFbyYhuDjwGRJi5QzOf
iu0TCa9uEtKUas610luihENZAQIiF7MRaL5XfmToU24=
3517262215D8D3008CBF888750B6418EDC4D562AC33ED6874E0D73ABA667BC3C
n2Au6L29UBBc2fEdbhtyAmTKpQRV7jQpdKVw+7Bcq8RzfUQmGwjEOtWTLTfPZXlx
M8X9pjLXmkUmNpxAUiXCS0VzRrfgsx47JCdWPtF77o1zbxjaTxGH9o3y3XsfapA3
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
VJibBREzYucPjNukhWG65jB60OIZQrcDVR3W2JV3G5ynshQ4Nd74pHrZYUgRiYK0
c103703e120ae8cc73c9248622f3cd1e
jLlOehpoNgAQzvuHrTyBcudcfwOhFguv/E47mcpJrto=
92974c6802419e4d18b5ec536cbfa167b8e8eff09ec4c8510a5b95750b1e0c82
pzhIFr8jSwvyB8FXK2qfBOfw0jXHNl6+dmbReaTm1jquB51r9sbZLlTA4zaBxZEm
49f946663a8deb7054212b8adda248c6
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
Do3k5DuMuAsRGeDxKZVVE8+FSftLk9ZlBUPdFxDzrUE=

POSSIBLE SECRETS
e2f856b9f9a4fd4cb2795aeaf83268e4bff189aaec05d691ffde76e075b82648
uVfRV2qL6y+/frn7UQ8HZUcJpLFj+yNt3k4Ns9czyDlwcIbIheGCFGCtGsGaaHh4
iH08ecr5p8p5eQT3/BFJ6jAaJm3eLNoIe2oA7hLZl5P0jAtinrUdPK16lrJGpxBz
B3EEABB8EE11C2BE770B684D95219ECB
f6040d0e807aaec325ecf44823765544e92905158169f694b282bf17388632cf95a83bae7d2d235c1f039b0df1dcca5fda619b6f7f459f2ff8d70ddb7b601592fe29fcae58c028f319b3b12495e67aa5390942a997a8cb572c8030b2df5c2b622608bea02b0c3e5d4dff3f72c9e3204049a45c0760cd3604af8d57f0e0c693cc
1GRZIGWaJCWi5hYVyOzM0ARje4NaXoHaW7HEe5QbRxs=
5fed96c85bd58c58aadbd465c172a4c9a794d8eb2f86cbc7bcee6caf4c7a2c5f
4230baa077b401374d0fc012375047e79ea0790d58d095ef18d97d95470c738d
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
xNZCZdqL8o1jZKUOIQXHHGKMYJmFGBT5z1mMXWF7VHR3erPGPRFl7DocpCFVg9bF
glZYRiAaVgXhfq7gmv5KdTlxK1u1W7CDU+wEOCdR48SsabliUSLxOyNuMGeUOQq8
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d010104050003820101006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
d80f18e8081b624cc64985f87f70118f1702985d2e10dbc985ee7be334fd3c7d
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
KFN28huBDzw/UNPPRO5YgG4GEIzzfegN1j75wmksmGk=

POSSIBLE SECRETS
RhEw32BK9OU3wzUC3Jj98VTZvnt6yWz3Jzx/x8tD2qo=
pJoEelkZiKPOxk90a9HaLYHjU9iyGURNQtyjZ4Eem1yb/gFTG2yLqZLPefEosnhY
IGAB4+J/PDJStxsBeRODYeAaV8Ap48L0bK2MK3UJNBs=
uUtXgghNropSfe2KUSoP0Efn1EgB4X6maOF+tPLLzG1rSS0RqDSE3s9EWbbdwRaZ
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
3Z4807bJ0KoyYYoQ9dcfmEBolGH5CdxZiQurF1neOqs=
8jFByxLLStK1ZA6Q/SQPKITUmXlRJfaQf0bJ+6rt27M=
24fbae40bcd50b759b26e3ba0f46aa25e932fa7da05f226d75ec507bcf53bce5
E5fWzXFb8RAG+0QVT91wIl5kQfApis+Ago2PTXmCPgE=
CIY4BMAyy7Fe28Pq7/h8od2SEEojcWEgmd3J7ORxssU=
9GRJeHWq4dh2BvJK4ycB7gT7rSPz0ZkF1/0dgXOpChUtvNoPNNrpav7wZxlsKwP4
BcJJ7m9GnDZ5QH3kvN4kRXKQduFKSe4hbLIA7qGtn8k=
HM4qeDzacgZSWStWAwQJTi2Amm6uvEB2WlZumyUY0B8=
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
wAGvvwsR6C1vDVsIyeUg+KWcunmHMDzvTAjP5mYaviw=
115792089210356248762697446949407573529996955224135760342422259061068512044369
hQ5xuCRMiz6eJqaT4+9Wf/Kj854Yma0NmQLTM8SLOoEkyUHQjbgUSxF3PTxTz3Bq
db48223fd9e143f7e133c57f5d08a4e38549ce3ebd921fe3b4003c26e5e35bed
b368b110e3b565fe97c91f786e11bc48754cc8e4e6f21d8a94a68ac6ad67aaaf
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
fI0N3kbZw/umjLZrsorw2Wh0+0tg4xypZfrKau+VpPGw8hjO0IIZVyJi5hB0Wcbt

POSSIBLE SECRETS
YnDH+tthutt98if0TMBwjusoYiZkXUV9qrwRfqxnS3g=
TiANcug5zndviERrHpzUihvZthrd+vHCK5ngnbrocVE=
07ff9b7aeeff969173c45b285fe0fecdbaae244576ff7a2796a36f1c0c11adb4
686479766013060971498190079908139321726943530014330540939446345918554318339765605212255964066145455497729631139148085803712198799971664381257402829111505715 1
PDJGtr7hH5z8kziZtOwKBHfUklGaxsnuMOcaf4/XJNQXH5uqgOnO+ZxxlrN1G5R2
e9702f1e92e97fce49cdf81a5fa730a4e913554d09b3fe41e1d8a7fba00a8459
403f14ad2f0e5eb3c4f3a0bcd5c1592cc4492662ad53191c92905255d4990656
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d0101040500308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d010104050003820101 0019d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
173cf86fe9894a0f70dadd09d4fd88c380836099d4939f8c3754361bdc16a32b
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
3081a0adab3018d57165e6dd24074bdbac640f6dbe21a9e24d3474a87ebf38b8
llxemQySqp4ImE2+K1SCPJZsWjXNCqydynC9yBT/03FiPJ85o8JSvF0iMBwiw5vV
Gvy6wet11FtrNaAWhnvYSI1hOQnkPBTAgqoI9PXuwaM=
INyd2w/uRsAGkjbqPl7ialNH5emmi1OBLIEI6gUyIzM=
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n

POSSIBLE SECRETS
dCN8M8R2yrrpg52x17w1rrrZtT0eIXPeEX6Ibp28VuQ=
db53fcdc9ab71e9bdd4eab257fe1aba7989ad2b24fbe3a85dfef72ea1dd6bae2
RbRyr5uGUYOSrOuNnmzV0kl42YeLvs7OFWbwh2MFm18=
B92825C2BD5D6D6D1E7F39EECD17843B7D9016F611136B75441BC6F4D3F00F05
SnrtMYC9+qStj9ZoSAj1DR6mGb7YlLFiZbsMn2F8wpevpQUtlzrwws7lBSZ1KQhS
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
nKg4HNqb3w+l+hWBt0181NzZuRHIlhptjDdMcQ5dE3JWGvySjoPYfybKeplgFTfD
E49D5C2C0E11B3B1B96CA56C6DE2A14EC7DAB5CCC3B5F300D03E5B4DBA44F539
4bdecdf772491e35c4e8b48f88aee22bae1311984f2e1da4dfad0b78ee7f5163
t7YLiNn9wSLVfNzBPSP796qGY15c9YWt19X86sjfqa1MN8DTMOAxKskDGE2b7plQ
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643

PLAYSTORE INFORMATION

Title: KidControl. Family GPS locator

Score: 3.6868687 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Social **Play Store URL:** ru.kidcontrol.gpstracker

Developer Details: KidControl Dev., 6687539553449035845, Saint-Petersburg, Zvenigorodskaya str. 22 191119 , https://kid-control.com, help@kid-control.com,

Release Date: May 31, 2015 **Privacy Policy:** Privacy link

Description:

Personal safety app keeps track of where your family members are. It's free! Family GPS tracker KidControl Circles - an app for the safety of your children and family. Your family can share their location, for example you can know where your child is when he left school. You can receive automatic notification when he arrives on its place. In GPS locator you can create separate circles for family. You will see them in your private account, on a separate map. Access to each circle is possible only by special invitation. In GPS locator you can: - add family members to your private account - create circles for private groups - create places-geofences and receive automatic notifications that a child has left or arrived at a place (e.g., a school) - browse the location history for today and yesterday - manage the rights of users in your account - hide or show your location to other users - see where a traceable phone might have gotten lost - the child can send an SOS signal in a difficult situation to all members of the circle You can always be in touch with your family and take parental control of your children You can create any circle for family and use it anytime or delete it when you don't need it. To get automated alerts when your kid arrives somewhere, create Places (Geo fences), such as School and Home. When your kid enters or leaves these areas, your phone receives a notification. Parents can see their child's movements online and always be sure they're all right. If a child gets lost or gets into a difficult situation, he can use the SOS button to send a help alert. In the Premium-version: - possibility to create unlimited number of circles and places - the ability to add unlimited number of users to each circle - movement and battery history during 2 weeks (instead 2 days in free). - Blackbox feature - recording of geodata when Internet is off To provide precise coordinates, the phone must have Location service enabled. Enabled Wi-Fi increases accuracy to 10-40 meters and works indoors. GPS location has accuracy of 10-50 meters, only outdoors. When GPS tracking and Wi-Fi location are turned off or not available, KidControl family locator determines phone's location by LBS coordinates of GSM towers. KidControl is not a spying or secret surveillance solution and the app can not be installed remotely or secretly. To join this service user has to install the app himself and enter the invitation code from the inviting user. Users have the option to stop sharing location for some time or log out from an account or completely delete the app. The app is visible in programs. Users can share location only inside one account.

SCAN LOGS

Timestamp	Event	Error
2024-08-11 12:47:32	Generating Hashes	OK
2024-08-11 12:47:32	Extracting APK	OK
2024-08-11 12:47:32	Unzipping	OK
2024-08-11 12:47:32	Getting Hardcoded Certificates/Keystores	OK
2024-08-11 12:47:35	Parsing AndroidManifest.xml	OK
2024-08-11 12:47:35	Parsing APK with androguard	OK
2024-08-11 12:47:35	Extracting Manifest Data	OK
2024-08-11 12:47:35	Performing Static Analysis on: KidControl Circles (ru.kidcontrol.gpstracker)	OK
2024-08-11 12:47:35	Fetching Details from Play Store: ru.kidcontrol.gpstracker	OK
2024-08-11 12:47:35	Manifest Analysis Started	OK
2024-08-11 12:47:36	Reading Network Security config from network_security_configuration.xml	OK
2024-08-11 12:47:36	Parsing Network Security config	OK
2024-08-11 12:47:36	Checking for Malware Permissions	OK

2024-08-11 12:47:36	Fetching icon path	OK
2024-08-11 12:47:36	Library Binary Analysis Started	OK
2024-08-11 12:47:36	Analyzing lib/armeabi-v7a/libapp.so	OK
2024-08-11 12:47:36	Analyzing lib/armeabi-v7a/libpbkdf2.so	OK
2024-08-11 12:47:36	Analyzing lib/armeabi-v7a/libTransform.so	OK
2024-08-11 12:47:36	Analyzing lib/armeabi-v7a/libucs-credential.so	OK
2024-08-11 12:47:36	Analyzing lib/armeabi-v7a/libflutter.so	OK
2024-08-11 12:47:37	Analyzing lib/x86_64/libapp.so	OK
2024-08-11 12:47:37	Analyzing lib/x86_64/libpbkdf2.so	OK
2024-08-11 12:47:37	Analyzing lib/x86_64/libucs-credential.so	OK
2024-08-11 12:47:37	Analyzing lib/x86_64/libflutter.so	OK
2024-08-11 12:47:37	Analyzing lib/arm64-v8a/libapp.so	OK
2024-08-11 12:47:37	Analyzing lib/arm64-v8a/libpbkdf2.so	OK
2024-08-11 12:47:37	Analyzing lib/arm64-v8a/libTransform.so	OK
2024-08-11 12:47:37	Analyzing lib/arm64-v8a/libucs-credential.so	OK

2024-08-11 12:47:37	Analyzing lib/arm64-v8a/libflutter.so	OK
2024-08-11 12:47:37	Analyzing lib/x86/libpbkdf2.so	OK
2024-08-11 12:47:38	Analyzing lib/x86/libucs-credential.so	OK
2024-08-11 12:47:38	Analyzing apktool_out/lib/armeabi-v7a/libapp.so	OK
2024-08-11 12:47:38	Analyzing apktool_out/lib/armeabi-v7a/libpbkdf2.so	OK
2024-08-11 12:47:38	Analyzing apktool_out/lib/armeabi-v7a/libTransform.so	OK
2024-08-11 12:47:38	Analyzing apktool_out/lib/armeabi-v7a/libucs-credential.so	OK
2024-08-11 12:47:38	Analyzing apktool_out/lib/armeabi-v7a/libflutter.so	OK
2024-08-11 12:47:38	Analyzing apktool_out/lib/x86_64/libapp.so	OK
2024-08-11 12:47:38	Analyzing apktool_out/lib/x86_64/libpbkdf2.so	OK
2024-08-11 12:47:38	Analyzing apktool_out/lib/x86_64/libucs-credential.so	OK
2024-08-11 12:47:38	Analyzing apktool_out/lib/x86_64/libflutter.so	OK
2024-08-11 12:47:39	Analyzing apktool_out/lib/arm64-v8a/libapp.so	OK
2024-08-11 12:47:39	Analyzing apktool_out/lib/arm64-v8a/libpbkdf2.so	OK
2024-08-11 12:47:39	Analyzing apktool_out/lib/arm64-v8a/libTransform.so	OK

2024-08-11 12:47:39	Analyzing apktool_out/lib/arm64-v8a/libucs-credential.so	OK
2024-08-11 12:47:39	Analyzing apktool_out/lib/arm64-v8a/libflutter.so	OK
2024-08-11 12:47:39	Analyzing apktool_out/lib/x86/libpbkdf2.so	OK
2024-08-11 12:47:39	Analyzing apktool_out/lib/x86/libucs-credential.so	OK
2024-08-11 12:47:39	Reading Code Signing Certificate	OK
2024-08-11 12:47:39	Running APKiD 2.1.5	OK
2024-08-11 12:47:43	Detecting Trackers	OK
2024-08-11 12:47:45	Decompiling APK to Java with jadx	OK
2024-08-11 12:48:02	Converting DEX to Smali	OK
2024-08-11 12:48:02	Code Analysis Started on - java_source	OK
2024-08-11 12:48:15	Android SAST Completed	OK
2024-08-11 12:48:15	Android API Analysis Started	OK
2024-08-11 12:48:23	Android Permission Mapping Started	OK
2024-08-11 12:48:33	Android Permission Mapping Completed	OK
2024-08-11 12:48:34	Finished Code Analysis, Email and URL Extraction	OK

2024-08-11 12:48:34	Extracting String data from APK	OK
2024-08-11 12:48:35	Extracting String data from SO	OK
2024-08-11 12:48:35	Extracting String data from Code	OK
2024-08-11 12:48:35	Extracting String values and entropies from Code	OK
2024-08-11 12:48:38	Performing Malware check on extracted domains	OK
2024-08-11 12:48:42	Saving to Database	OK

Report Generated by - MobSF v4.0.6

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