MOBSF

ANDROID STATIC ANALYSIS REPORT

Pingo (2.7.79-google)

File Name:	Google Play Store Apps_merged.apk
Package Name:	org.findmykids.child
Scan Date:	Aug. 11, 2024, 6:03 p.m.

App Security Score: 49/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	32	3	2	3

FILE INFORMATION

File Name: Google Play Store Apps_merged.apk
Size: 33.08MB
MD5: f759a909bff7e545eb9e938ec18c2be7
SHA1: 8c2aa6af823385408b7d6ca909b1217f218c2134
SHA256: 9e120bd84f0a72e25418c21bb7d7c9b8a893a0e9d40cc05e09530ae008e6f837

APP INFORMATION

App Name: Pingo
Package Name: org.findmykids.child
Main Activity: org.findmykids.app.presentation.screens.launcher.presentation.LauncherActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 2.7.79-google
Android Version Code: 2007790

APP COMPONENTS

Activities: 30
Services: 27
Receivers: 32
Providers: 10
Exported Activities: 2
Exported Services: 6
Exported Receivers: 13
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: L=Perm, CN=Nikolay Kuznetsov
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-05-04 16:16:19+00:00
Valid To: 2115-04-10 16:16:19+00:00
Issuer: L=Perm, CN=Nikolay Kuznetsov
Serial Number: 0x325856ba
Hash Algorithm: sha256
md5: 8839b094f67cf4c0ac7ed3b0dd635b63
sha1: 2a57777e3b9491a37392afce2e69d030dbf95037

sha256: 840b08c86d54e2f1da81e96c4b3e5d18e712921ad0e16257d9e6ea6817c24596
sha512: df94431212cf766e380dfa935c28f9dd27982cefd04727150c01c76c27456e7b53c104889f6c865b123318f365760ae7d341e2fb11fc4fda0fd53298147151bb
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 7a4f3805fc7d680574fd9f8698bc57bd27b79b31f8798fda722a7c093780b407
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
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_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.

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.
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_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
android.permission.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
android.permission.FOREGROUND_SERVICE_MICROPHONE	normal	permits foreground services with microphone use.	Allows a regular application to use Service.startForeground with the type "microphone".
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.FOREGROUND_SERVICE_SPECIAL_USE	normal	enables special-use foreground services.	Allows a regular application to use Service.startForeground with the type "specialUse".

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
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.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
org.findmykids.child.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MANUFACTURER check</td></tr><tr><td>Compiler</td><td>r8</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator check
network operator name check
ro.hardware check
ro.kernel.qemu check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
org.findmykids.app.presentation.screens.launcher.presentation.LauncherActivity	Schemes: fmk://, gmd://, https://, Hosts: @string/deeplink_domain, @string/branded_deeplink_domain,

ACTIVITY	INTENT
org.findmykids.app.presentation.screens.home.ChildHomeActivity	Schemes: tel://,
com.crowdin.platform.auth.AuthActivity	Schemes: crowdintest://,

NETWORK SECURITY

HIGH: 0 | WARNING: 0 | INFO: 0 | SECURE: 0

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 22 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	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	Activity (org.findmykids.app.presentation.screens.home.ChildHomeActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Broadcast Receiver (org.findmykids.app.presentation.receivers.RingModeBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Broadcast Receiver (org.findmykids.core.antiremoval.child.impl.data.ChildDeviceAdminReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_DEVICE_ADMIN [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
6	Service (org.findmykids.callscreening.child.ChildCallScreeningService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_SCREENING_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
7	Broadcast Receiver (org.findmykids.callscreening.child.missedCalls.presentation.PhoneStateReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Service (org.findmykids.pushes.google.FcmListenerService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Service (pro.userx.server.job.ApiJobService) 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	Service (org.findmykids.logSend.presentation.services.LogSendJobService) 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.
11	Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.SleepEventReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.ACTIVITY_RECOGNITION [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.
12	Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.BootReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.RECEIVE_BOOT_COMPLETED [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
13	Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.PassiveReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.ActivityReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
15	Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.PassiveFusedReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
16	Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.StationReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
17	Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.ActivityEventReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.ACTIVITY_RECOGNITION [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.
18	Service (org.findmykids.geo.producer.presentation.service.BootJobSchedulerService) 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.
19	Activity (com.crowdin.platform.auth.AuthActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
20	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.
21	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.

NO	ISSUE	SEVERITY	DESCRIPTION
22	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.
23	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **2** | WARNING: **8** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/airbnb/lottie/LottieAnimationView.java com/appsflyer/internal/AFf1cSDK.java com/appsflyer/internal/AFf1fSDK.java com/appsflyer/internal/AFf1gSDK.java com/appsflyer/internal/AFf1uSDK.java com/appsflyer/internal/AFg1dSDK.java com/appsflyer/share/LinkGenerator.java com/bumptech/glide/a.java com/crowdin/platform/Crowdin.java com/crowdin/platform/CrowdinConfig.java com/crowdin/platform/ShakeDetectorManager.java com/crowdin/platform/auth/AuthActivity.java com/crowdin/platform/data/DataManager.java com/crowdin/platform/data/remote/CrowdingRepository$getManifest$1.java com/crowdin/platform/data/remote/CrowdingRepository.java com/crowdin/platform/data/remote/DistributionInfoManager.java com/crowdin/platform/data/remote/MappingRepository.java com/crowdin/platform/data/remote/StringDataRemoteRepository.java com/crowdin/platform/data/remote/TranslationDataRepository$getFiles$1.java com/crowdin/platform/data/remote/TranslationDataRepository.java com/crowdin/platform/realtimeupdate/EchoWebSocketListener.java com/crowdin/platform/realtimeupdate/RealTimeUpdateManager.java com/crowdin/platform/screenshot/ScreenshotService.java com/crowdin/platform/util/ExtensionsKt.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/crowdin/platform/util/ExtensionsKt.java com/intercom/twig/Twig.java defpackage/a0c.java defpackage/a5b.java defpackage/a71.java defpackage/ah3.java defpackage/an3.java defpackage/anb.java defpackage/ap9.java defpackage/aq.java defpackage/au2.java defpackage/b09.java defpackage/b75.java defpackage/bc9.java defpackage/be3.java defpackage/bk1.java defpackage/by0.java defpackage/c68.java defpackage/ck7.java defpackage/cnb.java defpackage/cob.java defpackage/cu5.java defpackage/cv.java defpackage/cv0.java defpackage/cv2.java defpackage/cw4.java defpackage/cx7.java defpackage/d39.java defpackage/d4c.java defpackage/d63.java defpackage/d7.java defpackage/df9.java defpackage/dg2.java defpackage/dq6.java defpackage/ds4.java defpackage/dxb.java defpackage/e09.java defpackage/e38.java defpackage/e9b.java defpackage/eg7.java defpackage/eg9.java defpackage/eh1.java defpackage/ek4.java defpackage/ek8.java defpackage/el9.java defpackage/ep8.java defpackage/et9.java defpackage/eu4.java defpackage/ev2.java defpackage/f6.java defpackage/fc3.java defpackage/fd3.java defpackage/fi7.java defpackage/fk9.java defpackage/fl7.java defpackage/fq3.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	defpackage/ft8.java defpackage/fu9.java defpackage/g1b.java defpackage/g22.java defpackage/g25.java defpackage/g39.java defpackage/g45.java defpackage/gc3.java defpackage/gd1.java defpackage/ge3.java defpackage/ge7.java defpackage/gk8.java defpackage/gl1.java defpackage/gqa.java defpackage/h3b.java defpackage/h81.java defpackage/h9b.java defpackage/hb6.java defpackage/he0.java defpackage/hg3.java defpackage/hk5.java defpackage/hl1.java defpackage/hmb.java defpackage/hp.java defpackage/hq1.java defpackage/hua.java defpackage/hva.java defpackage/i09.java defpackage/ikb.java defpackage/ip.java defpackage/iu4.java defpackage/ix7.java defpackage/ixa.java defpackage/iy7.java defpackage/iyb.java defpackage/j15.java defpackage/j67.java defpackage/ja7.java defpackage/jb3.java defpackage/jd1.java defpackage/je0.java defpackage/jf7.java defpackage/ji2.java defpackage/jk5.java defpackage/jo3.java defpackage/jr9.java defpackage/k09.java defpackage/k15.java defpackage/ke0.java defpackage/ky.java defpackage/l23.java defpackage/l4c.java defpackage/lc5.java defpackage/ld3.java defpackage/le5.java defpackage/lmb.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/lp2.java defpackage/lt9.java defpackage/lu5.java defpackage/lu8.java defpackage/lx7.java defpackage/m11.java defpackage/m70.java defpackage/mf8.java defpackage/mi7.java defpackage/mq9.java defpackage/mr4.java defpackage/mu4.java defpackage/mva.java defpackage/n10.java defpackage/n2c.java defpackage/n30.java defpackage/n3b.java defpackage/n49.java defpackage/n62.java defpackage/nh1.java defpackage/nj5.java defpackage/np8.java defpackage/nr9.java defpackage/nt0.java defpackage/nxa.java defpackage/o42.java defpackage/o51.java defpackage/o7.java defpackage/oc.java defpackage/od3.java defpackage/okb.java defpackage/olb.java defpackage/on2.java defpackage/os1.java defpackage/ot2.java defpackage/ox7.java defpackage/p4.java defpackage/p5.java defpackage/pf7.java defpackage/ps3.java defpackage/pv9.java defpackage/px4.java defpackage/q01.java defpackage/qdb.java defpackage/qr1.java defpackage/qs9.java defpackage/qua.java defpackage/qx4.java defpackage/r7b.java defpackage/rc5.java defpackage/rc8.java defpackage/rea.java defpackage/rj9.java defpackage/rpa.java defpackage/rs9.java defpackage/rt9.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/ru1.java defpackage/s68.java defpackage/sb3.java defpackage/sf7.java defpackage/so5.java defpackage/sq2.java defpackage/sq6.java defpackage/t10.java defpackage/t70.java defpackage/td1.java defpackage/tn4.java defpackage/tr6.java defpackage/tta.java defpackage/tv9.java defpackage/ty8.java defpackage/u2c.java defpackage/u45.java defpackage/u4c.java defpackage/u9.java defpackage/ub.java defpackage/uc5.java defpackage/uo.java defpackage/uo5.java defpackage/uq9.java defpackage/uqa.java defpackage/uqb.java defpackage/uwb.java defpackage/ux4.java defpackage/uya.java defpackage/uzb.java defpackage/v6b.java defpackage/vb9.java defpackage/vg3.java defpackage/vi8.java defpackage/vl9.java defpackage/vp4.java defpackage/vpa.java defpackage/w3c.java defpackage/wc2.java defpackage/wc5.java defpackage/wmb.java defpackage/wua.java defpackage/wxa.java defpackage/x2c.java defpackage/x6.java defpackage/x6b.java defpackage/xb9.java defpackage/xlb.java defpackage/xsa.java defpackage/xv0.java defpackage/xya.java defpackage/y11.java defpackage/y5.java defpackage/y7.java defpackage/yg8.java defpackage/yk3.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/ysa.java defpackage/yx4.java defpackage/yy9.java defpackage/z1a.java defpackage/z53.java defpackage/z63.java defpackage/zb3.java defpackage/zf.java defpackage/zn5.java defpackage/zo9.java
2	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/crowdin/platform/CrowdinPreferences.java com/crowdin/platform/data/local/SharedPrefLocalRepository.java defpackage/fk9.java defpackage/k4.java defpackage/oq3.java defpackage/tq6.java defpackage/wn6.java defpackage/xp4.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	defpackage/b26.java defpackage/gh6.java defpackage/ha0.java defpackage/jaa.java defpackage/k71.java defpackage/k79.java
4	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/appsflyer/internal/AFb1gSDK.java com/appsflyer/internal/AFc1iSDK.java defpackage/a38.java defpackage/do2.java defpackage/gc6.java defpackage/gi6.java defpackage/h9b.java defpackage/sz5.java defpackage/ts1.java defpackage/um2.java defpackage/uw9.java defpackage/v2.java defpackage/v57.java
5	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	defpackage/ah3.java defpackage/dq5.java defpackage/yr.java defpackage/zo.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	com/crowdin/platform/data/model/AuthConfig.java com/crowdin/platform/data/model/RefreshToken.java com/crowdin/platform/data/model/StringData.java com/crowdin/platform/data/model/TokenRequest.java defpackage/cd2.java defpackage/ci1.java defpackage/e86.java defpackage/ec9.java defpackage/f00.java defpackage/g65.java defpackage/hc5.java defpackage/lz1.java defpackage/mv.java defpackage/n26.java defpackage/nz.java defpackage/rn2.java defpackage/s78.java defpackage/u25.java defpackage/ye7.java defpackage/z00.java defpackage/z16.java
7	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	defpackage/fl7.java defpackage/jk5.java defpackage/le6.java defpackage/rga.java defpackage/sc8.java
8	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	defpackage/gu0.java
9	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	org/findmykids/app/presentation/screens/finishtask/WebTaskActivity.java org/findmykids/app/presentation/screens/finishtask/web/WebTaskFragment.java org/findmykids/app/presentation/screens/web/WebFullActivity.java
10	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	defpackage/im7.java defpackage/qe4.java defpackage/sh1.java defpackage/up7.java defpackage/y63.java
11	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	defpackage/an3.java defpackage/maa.java defpackage/wj0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	defpackage/j4c.java defpackage/maa.java defpackage/qmb.java defpackage/wy0.java
13	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	defpackage/onb.java
14	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	defpackage/el9.java
15	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	defpackage/jaa.java

SHARED LIBRARY BINARY ANALYSIS

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	x86_64/libdatastore_shared_counter.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.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/24	android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECORD_AUDIO, android.permission.SYSTEM_ALERT_WINDOW, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.READ_CONTACTS, android.permission.READ_PHONE_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	9/45	android.permission.CHANGE_WIFI_STATE, android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.ACTIVITY_RECOGNITION, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.PACKAGE_USAGE_STATS, android.permission.ACTIVITY_RECOGNITION, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.

Other Common Permissions:
Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
www.baidu.com	IP: 103.235.46.96 Country: Hong Kong Region: Hong Kong City: Hong Kong

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
sattr.s	ok	No Geolocation information available.
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
schemas.microsoft.com	ok	**IP:** 13.107.246.60 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
sadrevenue.s	ok	No Geolocation information available.
gdemoideti.onelink.me	ok	**IP:** 13.32.110.57 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
.facebook.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
ya.ru	ok	**IP:** 77.88.55.242 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
geoapi.findmykids.org	ok	**IP:** 185.104.209.16 **Country:** Czechia **Region:** Karlovarsky kraj **City:** Mesto **Latitude:** 49.979969 **Longitude:** 12.864320 **View:** Google Map
console.userx.pro	ok	**IP:** 104.22.14.140 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.baidu.com	ok	**IP:** 103.235.46.96 **Country:** Hong Kong **Region:** Hong Kong **City:** Hong Kong **Latitude:** 22.285521 **Longitude:** 114.157692 **View:** Google Map
developers.facebook.com	ok	**IP:** 31.13.84.8 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
firebase.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

DOMAIN	STATUS	GEOLOCATION
pagead2.googlesyndication.com	ok	**IP:** 142.251.208.98 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
sapp.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.
google.com	ok	**IP:** 142.251.208.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.
graph.s	ok	No Geolocation information available.
www.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
scdn-stestsettings.s	ok	No Geolocation information available.
where-is-my-children.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sconversions.s	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.
app-measurement.com	ok	**IP:** 142.250.180.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
243408.selcdn.ru	ok	**IP:** 92.53.68.16 **Country:** Russian Federation **Region:** Sankt-Peterburg **City:** Saint Petersburg **Latitude:** 59.894440 **Longitude:** 30.264170 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.251.39.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.15.200 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 142.250.201.195 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
graph-video.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
svalidate-and-log.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.
sviap.s	ok	No Geolocation information available.
svalidate.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
aps-webhandler.appsflyer.com	ok	**IP:** 3.165.206.56 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
facebook.com	ok	**IP:** 31.13.84.36 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
aomedia.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
ssdk-services.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
sars.s	ok	No Geolocation information available.
g.co	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
simpression.s	ok	No Geolocation information available.
distributions.crowdin.net	ok	**IP:** 3.165.206.13 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
default.url	ok	No Geolocation information available.
developer.android.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
api.crowdin.com	ok	**IP:** 44.212.243.122 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
accounts.crowdin.com	ok	**IP:** 54.209.15.179 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
goo.gle	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
sinapps.s	ok	No Geolocation information available.

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://where-is-my-children.firebaseio.com/.json	high Firebase DB is exposed publicly.

EMAILS

EMAIL	FILE
u0013android@android.com u0013android@android.com0	defpackage/dob.java

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"pingo_first_session_terms_got_it" : "Fortsett"
"first_session_pingo_dialog_desc_son_with_name_4" : "□□□□□□□□□%s□□□□□□"
"cross_auth_email_not_translateable" : "E-mail"
"first_session_pingo_achive_action" : "□!"
"pingo_first_session_terms_got_it" : "Продължи"
"pingo_first_session_terms_got_it" : "Nadaljuj"
"pingo_first_session_lets_go" : "Start!"
"step_connection_description_for_parent_user" : "□□□□"
"step_connection_description_for_parent_user" : "szülőknek"
"cross_auth_email" : "Почта"
"first_session_pingo_dialog_desc_son_with_name_5" : "%s□□□□□□□□□□□□"
"pingo_first_session_lets_go" : "Aloitetaan!"
"step_connection_description_for_parent_user" : "Lapsevanemale"
"cross_auth_set_email" : "E□□□□□□"
"pingo_first_session_terms_got_it" : "Настави"

POSSIBLE SECRETS
"pingo_first_session_terms_got_it" : "Kontynuuj"
"cross_auth_units_email_title" : "Почта"
"cross_auth_code_sent_title" : "□□□□□□□□□"
"pingo_first_session_terms_got_it" : "Seguinte"
"first_session_pingo_dialog_desc_1" : "□□□□□□□□□□□□□□□□"
"firebase_database_url" : "https://where-is-my-children.firebaseio.com"
"pingo_first_session_terms_got_it" : "Далі"
"step_connection_description_for_parent_user" : "Vanhemmalle"
"step_connection_description_for_child_user" : "Gyereknek"
"pingo_first_session_role_child" : "لنفسي"
"first_session_pingo_dialog_desc_daughter_with_name_4" : "□□□□□□□□□□□□□%s□□□□□□□"
"step_connection_description_for_child_user" : "□□□□"
"pingo_first_session_lets_go" : "Início"
"cross_auth_code_sent_title" : "□□□□E□□□□□□"
"pingo_first_session_lets_go" : "□□"
"pingo_first_session_accept_terms" : "□□□□□□□□□□□□□□□□□□□□□□□□[terms_link]□□□□[/terms_link]□[policy_link]□□□□[/policy_link]"
"cross_auth_email" : "□□□□"
"cross_auth_units_email_title" : "□□□□"
"cross_auth_units_email_title" : "■-■■■"
"cross_auth_units_email_title" : "E□□□"
"step_connection_description_for_parent_user" : "□□□□"
"cross_auth_email" : "Имейл"

POSSIBLE SECRETS
"cross_auth_units_email_title" : "Sähköposti"
"pingo_first_session_lets_setup_your_phone" : "[redacted]"
"pingo_first_session_who_are_you" : "□□□□□□□□□□□□□"
"pingo_first_session_terms_got_it" : "Doorgaan"
"cross_auth_email" : "Email"
"pingo_first_session_terms_got_it" : "Nastavak"
"pingo_first_session_lets_go" : "Kezdet!"
"first_session_pingo_dialog_desc_1" : "□□□□□□□□□□□□□□□□□□"
"cross_auth_units_email_title" : "E-адреса"
"pingo_first_session_terms_got_it" : "Pokračovat"
"pingo_first_session_age_title" : "□□□□□"
"first_session_pingo_achive_action" : "Иэ!"
"intercom_article_single_author" : "□□□{author_first_name}"
"step_connection_description_for_parent_user" : "[redacted]"
"pingo_first_session_terms_got_it" : "Jätka"
"pingo_first_session_role_child" : "Nekem"
"pingo_first_session_terms_got_it" : "استمرار"
"cross_auth_units_email_title" : "E-Mail-Adresse"
"step_connection_description_for_parent_user" : "□□□□"
"step_connection_description_for_child_user" : "Lapselle"
"pingo_first_session_terms_got_it" : "Weiter"
"pingo_first_session_terms_got_it" : "□□□"

POSSIBLE SECRETS
"cross_auth_email" : "[redacted]"
"pingo_first_session_call_parent_v2" : "□□□□□□□□□□□□□□□"
"pingo_first_session_lets_go" : "شروع"
"cross_auth_email" : "ایمیل"
"pingo_first_session_terms_got_it" : "Жалғастыру"
"pingo_first_session_role_child" : "Мне"
"cross_auth_units_email_title" : "E-mail"
"pingo_first_session_terms_got_it" : "□□"
"first_session_pingo_dialog_desc_daughter_with_name_5" : "%s□□□□□□□□□□□□□□□"
"com.google.firebase.crashlytics.mapping_file_id" : "56d6de7eae214cd5af57fc7ae3b0bda1"
"pingo_first_session_terms_got_it" : "Turpināt"
"step_connection_description_for_child_user" : "□□□"
"first_session_pingo_dialog_choose_avatar_camera" : "□□□□□□"
"pingo_first_session_terms_got_it" : "Συνέχεια"
"live_stopped_reason_secret" : "Salaisuudet"
"intercom_article_double_author" : "□□□□{author_first_name1}□{author_first_name2}"
"pingo_first_session_lets_go" : "□□□□"
"cross_auth_email" : "E-Mail-Adresse"
"live_stopped_reason_secret" : "□□□□"
"pingo_first_session_role_child" : "□□"
"pingo_first_session_terms_got_it" : "Continue"
"pingo_first_session_terms_got_it" : "Devam"

POSSIBLE SECRETS
"cross_auth_units_email_title" : "[redacted]"
"pingo_first_session_role_child" : "בשבילי"
"live_stopped_reason_secret" : "Rahasia"
"pingo_first_session_role_parent" : "Lapselleni"
"pingo_first_session_terms_got_it" : "□□"
"pingo_first_session_lets_go" : "Spustit!"
"cross_auth_email" : "אימייל"
"pingo_first_session_call_parent_v2" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"pingo_first_session_lets_go" : "Mulai"
"pingo_first_session_role_child" : "□"
"cross_auth_units_email_title" : "Имейл"
"pingo_first_session_lets_go" : "[redacted]"
"pingo_first_session_terms_got_it" : "[redacted]"
"step_connection_description_for_child_user" : "[redacted]"
"pingo_first_session_role_parent" : "□□□□□"
"pingo_first_session_age_title" : "□□□□□"
"google_api_key" : "AIzaSyDZp3fcu7xmJyoAHTFhQR5t47-W-4HNpOY"
"step_connection_description_for_child_user" : "Lapsele"
"step_connection_description_for_child_user" : "Bērnam"
"cross_auth_email" : "E-адреса"
"pingo_first_session_lets_go" : "Başlayın"
"pingo_first_session_lets_go" : "Уперед!"

POSSIBLE SECRETS
"pingo_first_session_lets_go" : "!מתחילים"
"first_session_pingo_dialog_desc_son_with_name_4" : "□□□□□□□□□□□□□□%s□□□□□□□□"
"first_session_pingo_dialog_desc_5" : "□□□□□□□□□□□□□□□□□□□□"
"pingo_first_session_role_child" : "Zame"
"pingo_first_session_terms_got_it" : "Продолжить"
"pingo_first_session_who_are_you" : "□□□□□□□□□□□□□"
"first_session_pingo_dialog_choose_avatar_gallery" : "□□□□□□□"
"cross_auth_email" : "■■■■"
"pingo_first_session_terms_got_it" : "המשך"
"pingo_first_session_age_title" : "□□□□□□□"
"step_connection_description_for_child_user" : "□□□□"
"pingo_first_session_lets_go" : "Pradėti"
"pingo_first_session_terms_got_it" : "Vazhdo"
"first_session_pingo_dialog_choose_avatar_camera" : "□□□□"
"pingo_first_session_lets_go" : "Fillo"
"cross_auth_units_email_title" : "E-post"
"pingo_first_session_terms_got_it" : "ادامه"
"cross_auth_email" : "E□□□"
"first_session_pingo_dialog_desc_son_with_name_5" : "%s□□□□□□□□□□□□□□□□"
"step_connection_description_for_parent_user" : "Vecākam"
"pingo_first_session_lets_go" : "Start"
"pingo_first_session_lets_go" : "Zaczynajmy"

POSSIBLE SECRETS
"pingo_first_session_terms_got_it" : "Continuer"
"first_session_pingo_achive_action" : "□□□"
"pingo_first_session_role_child" : "Minulle"
"step_connection_description_for_child_user" : "Vaikui"
"pingo_first_session_role_parent" : "■■■■■■■■■■■■"
"cross_auth_email" : "E-poçt"
"cross_auth_set_email" : "□□□□□□□"
"pingo_first_session_terms_got_it" : "Fortsæt"
"pingo_first_session_accept_terms" : "□□□□□□□□□□□□□□□□□□□□□□[terms_link]□□□□[/terms_link]□[policy_link]□□□□[/policy_link]"
"step_connection_description_for_parent_user" : "□□□□□□□"
"first_session_pingo_achive_action" : "■■■■■"
"pingo_first_session_terms_got_it" : "Continua"
"pingo_first_session_role_parent" : "□□□□□□"
"live_stopped_reason_secret" : "□□□□□"
"pingo_first_session_lets_go" : "Басталуы"
"cross_auth_units_email_title" : "E-pasts"
"pingo_first_session_terms_got_it" : "Fortsätt"
"pingo_first_session_lets_go" : "Sākums"
"first_session_pingo_dialog_desc_5" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"pingo_first_session_role_child" : "■■■■■■■"
"pingo_first_session_role_parent" : "□□□□□□□"
"pingo_first_session_terms_got_it" : "Lanjutkan"

POSSIBLE SECRETS
"live_stopped_reason_secret" : "Privatgespräch"
"step_connection_description_for_parent_user" : "להורה"
"first_session_pingo_achive_action" : "Evet!"
"first_session_pingo_dialog_choose_avatar_gallery" : "[redacted]"
"pingo_first_session_lets_go" : "Štart"
"first_session_pingo_dialog_choose_avatar_camera" : "□□□□"
"cross_auth_units_email_title" : "E-poçt"
"pingo_first_session_terms_got_it" : "□□"
"first_session_pingo_dialog_choose_avatar_camera" : "[redacted]"
"cross_auth_units_email_title" : "Mejladress"
"cross_auth_email" : "E-post"
"cross_auth_email" : "E-mail"
"first_session_pingo_dialog_desc_1" : "□□□□□□□□□□□□□□□"
"pingo_first_session_role_child" : "□□□□□"
"cross_auth_units_email_title" : "Email"
"pingo_first_session_role_parent" : "لطفلي"
"intercom_article_single_author" : "□□□□{author_first_name}"
"pingo_first_session_lets_setup_your_phone" : "□□□□□□□□□□□□□□□□□□□□□"
"first_session_pingo_dialog_desc_daughter_with_name_4" : "□□□□□□□□□%s□□□□□□"
"google_crash_reporting_api_key" : "AIzaSyDZp3fcu7xmJyoAHTFhQR5t47-W-4HNpOY"
"step_connection_description_for_child_user" : "لطفل"
"cross_auth_units_email_title" : "ايميل"

POSSIBLE SECRETS
"first_session_child_here" : "%s□□□□□□□□"
"cross_auth_set_email" : "[redacted]"
"first_session_pingo_dialog_desc_1" : "[redacted]"
"pingo_first_session_role_child" : "□□□"
"first_session_pingo_achive_action" : "□□□□□□□"
"intercom_article_multiple_authors" : "□□□□{author_first_name1}□□{number_of_other_authors}□"
"pingo_first_session_lets_go" : "البداية"
"pingo_first_session_who_are_you" : "[redacted]"
"cross_auth_units_email_title" : "E-posta"
"pingo_first_session_call_parent_v2" : "□□□□□□□□□□□□□□□"
"first_session_pingo_dialog_desc_4" : "□□□□□□□□□□□□□□□□□□□□□"
"pingo_first_session_lets_go" : "□□"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_terms_got_it" : "Jatka"
"cross_auth_code_sent_title" : "[redacted]"
"intercom_article_double_author" : "□□□{author_first_name1}□{author_first_name2}"
"live_stopped_reason_secret" : "□□□□"
"live_stopped_reason_secret" : "Salajutt"
"pingo_first_session_lets_go" : "Začni"
"pingo_first_session_call_parent_v2" : "[redacted]"
"pingo_first_session_lets_go" : "Почетак"
"pingo_first_session_lets_go" : "Početak!"

POSSIBLE SECRETS
"pingo_first_session_lets_go" : "Начало!"
"first_session_pingo_dialog_choose_avatar_camera" : "Kamera"
"first_session_pingo_dialog_desc_5" : "□□□□□□□□□□□□□□□□□□□□"
"pingo_first_session_age_title" : "■■■■■■■■■■■■"
"cross_auth_email" : "□□□"
"pingo_first_session_lets_setup_your_phone" : "□□□□□□□□□□□□□□□□"
"pingo_first_session_lets_go" : "Begin"
"step_connection_description_for_parent_user" : "Tėčiui/Mamai"
"pingo_first_session_lets_go" : "■■■"
"first_session_pingo_dialog_desc_5" : "□□□□□□□□□□□□□□□□□□"
"pingo_first_session_terms_got_it" : "Tovább"
"cross_auth_email" : "Mejladress"
"pingo_first_session_lets_go" : "Starta"
"step_connection_description_for_child_user" : "□□□□□□□□"
"pingo_first_session_terms_got_it" : "Tęsti"
"pingo_first_session_lets_go" : "Algus!"
"pingo_first_session_who_are_you" : "□□□□□□□□□□□□□□□□□□"
"cross_auth_units_email_title" : "אימייל"
"cross_auth_email" : "E-posta"
"pingo_first_session_terms_got_it" : "Continuați"
"pingo_first_session_terms_got_it" : "Pokračovať"
"pingo_first_session_lets_go" : "¡Vamos!"

POSSIBLE SECRETS
"pingo_first_session_lets_setup_your_phone" : "□□□□□□□□□□□□□□"
"step_connection_description_for_child_user" : "לילד"
"first_session_pingo_dialog_desc_daughter_with_name_5" : "%s□□□□□□□□□□□□□□"
"pingo_first_session_lets_go" : "¡Comencemos!"
"first_session_pingo_dialog_desc_4" : "□□□□□□□□□□□□□□□□□□□□□□"
"pingo_first_session_lets_go" : "Iniziamo!"
"pingo_first_session_lets_go" : "Έναρξη"
"intercom_api_key" : "android_sdk-b0ef5c43427c5301aa4f5c20bfcf4ca09b831d18"
"cross_auth_email" : "Sähköposti"
"first_session_pingo_dialog_desc_4" : "□□□□□□□□□□□□□□□□□□□□□□□□"
"cross_auth_units_email_title" : "□□□"
"first_session_pingo_dialog_choose_avatar_camera" : "Fotografuokite"
"cross_auth_email" : "E-pasts"
"pingo_first_session_role_child" : "Man"
"pingo_first_session_lets_go" : "Вперёд!"
"first_session_pingo_dialog_choose_avatar_gallery" : "□□□□□□□□□□"
756a18d015469157deb45aebd697eebd
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
afa8e68cdece85976f8a5a23b7db7774
0485de78a473be2850e99f865c0d331f
cc2751449a350f668590264ed76692694a80308a
c56fb7d591ba6704df047fd98f535372fea00211

POSSIBLE SECRETS
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
487914b203b2f98fccba43354c8a6842
5c725da8dd55f8c8c8aa5f46159b1e4f
470fa2b4ae81cd56ecbcda9735803434cec591fa
5bae185a7c59e709594f0bab1df18a2f
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
5abf736af0deb16fa07301cb99e10d16
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
128-c20968b22ed168a498a4bf28ebadc7e883bd4b8c2dba719cb4c661a2c15147f5
da742c954d1b019c0e8c3a7eb4e40ca2
b75577c96513ab2b3ef7ded18a2f0cf9
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
1497fe6d3ff464258f448d2ac6ce035f
d9ea72d42a1d9dd96c2b97d7ceb62d23
9b8f518b086098de3d77736f9458a3d2f6f95a37
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
2008dffa-cb3d-4010-a561-8f0f52d6dcea
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
7d73d21f1bd82c9e5268b6dcf9fde2cb
e11bf873f6121328882f2b346daba386

POSSIBLE SECRETS
566e3549904594cfc9dd2f45057b5ac5
b9834b3d46890f94943f52ad737044f5
183f065fcccfc7c869823cd02c1a83cd
c3096904ceec43e255c6377f39a98090
d3d0540467196ca8019ea490f662fdc1
e6c56e937ff46fd1b27376a92e0edef5
3071c8717539de5d5353f4c8cd59a032
c3de0c6ed63f95b0fb7274d6d08c0d91
babf943b8fa1846923c692445e518b96
676c7c7dddfd5985317ff4d7d77f1d1e
1634ac8041e59a0eeb107dcc6e33bfa4

PLAYSTORE INFORMATION

Title: Pingo by Findmykids

Score: 4.7288136 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Social **Play Store URL:** org.findmykids.child

Developer Details: GEO TRACK TECHNOLOGIES INC, 6976318052361578107, 8 The Green, Ste A, Dover, DE, 19901, http://findmykids.org, support@findmykids.org,

Release Date: Mar 7, 2018 **Privacy Policy:** Privacy link

Description:

Pingo is a companion app to the Findmykids location tracker, our app for parents. It was developed for location tracking of children. Please only install this location tracker app on a device used by a child or teenager. We recommend you start by downloading the Findmykids parent tracker app on your phone. After that, install the Pingo GPS location tracker on your child's device and enter the code from the Findmykids app you received when you signed up. Done! Now you can use kids GPS tracker! OUR KEY FEATURES: Kids GPS tracker – see your child's location on the map and the history of the day's activity - an online location diary. Make sure that your child does not go to dangerous places with our locator. You can also get your child a kid smart watch and connect it to the Pingo app. Sound around – listen to what's going on around your child with the help of our location tracker to make sure they're okay. This feature works only if the child tracker is installed and set up on their phone. Loud signal – send a loud signal to your child's phone where the child tracker is installed if they have left it in their backpack or on silent mode and can't hear the call. If they lose kid smart watch, you can also find them with the help of our GPS watch tracking app. Screen time manager – find out what apps they used at school, and whether they played in class instead of learning. Pingo kids GPS tracker can be used instead of any parental control apps. Notifications – make sure your child is on time for school: get notifications when they get to school, back home, and other places you've created. Our parent tracker app will send you a notification. Battery control – remind your child to charge the phone on time: you will be notified if the battery is about to run out. The feature also works with kid smart watch and GPS watch tracking app Family chat – chat with your child in the chat room with fun stickers and send voice messages in the child tracker app You can see your child's online location for free once the devices are connected. Other features in the free version (like parental control app for child phone) are available with restrictions. To use all the features of the app, you should buy a subscription. If your child doesn't have a phone, you can buy a kid smart watch and connect them to our GPS watch tracking app. GPS family tracker asks for the following permissions: – access to the camera and photos – to install the child's avatar; – access to contacts – to fill in the phone book in the GPS watch; – access to a microphone – to send voice messages in the chat; – accessibility services - to limit time at the smartphone screen. In case of technical problems with our parent tracker app, you can always contactFindmykids 24-hour support via support chat in the app or

by e-mail support@findmykids.org

SCAN LOGS

Timestamp	Event	Error
2024-08-11 18:03:27	Generating Hashes	OK
2024-08-11 18:03:27	Extracting APK	OK
2024-08-11 18:03:27	Unzipping	OK
2024-08-11 18:03:27	Getting Hardcoded Certificates/Keystores	OK
2024-08-11 18:03:31	Parsing AndroidManifest.xml	OK
2024-08-11 18:03:31	Parsing APK with androguard	OK
2024-08-11 18:03:34	Extracting Manifest Data	OK
2024-08-11 18:03:34	Performing Static Analysis on: Pingo (org.findmykids.child)	OK
2024-08-11 18:03:34	Fetching Details from Play Store: org.findmykids.child	OK
2024-08-11 18:03:34	Manifest Analysis Started	OK
2024-08-11 18:03:34	Reading Network Security config from network_security_config.xml	OK
2024-08-11 18:03:34	Parsing Network Security config	OK

2024-08-11 18:03:34	Checking for Malware Permissions	OK
2024-08-11 18:03:34	Fetching icon path	OK
2024-08-11 18:03:35	Library Binary Analysis Started	OK
2024-08-11 18:03:35	Analyzing lib/x86_64/libdatastore_shared_counter.so	OK
2024-08-11 18:03:35	Analyzing apktool_out/lib/x86_64/libdatastore_shared_counter.so	OK
2024-08-11 18:03:35	Reading Code Signing Certificate	OK
2024-08-11 18:03:35	Failed to get signature versions	CalledProcessError(1, ['/jdk-20.0.2/bin/java', '-Xmx1024M', '-Djava.library.path=', '-jar', '/home/mobsf/Mobile-Security-Framework-MobSF/mobsf/StaticAnalyzer/tools/apksigner.jar', 'verify', '--verbose', '/home/mobsf/.MobSF/uploads/f759a909bff7e545eb9e938ec18c2be7/f759a909bff7e545eb9e938ec18c2be7.apk'])
2024-08-11 18:03:35	Running APKiD 2.1.5	OK
2024-08-11 18:03:39	Detecting Trackers	OK
2024-08-11 18:03:42	Decompiling APK to Java with jadx	OK
2024-08-11 18:04:16	Converting DEX to Smali	OK
2024-08-11 18:04:16	Code Analysis Started on - java_source	OK
2024-08-11 18:05:13	Android SAST Completed	OK
2024-08-11 18:05:13	Android API Analysis Started	OK

2024-08-11 18:06:03	Android Permission Mapping Started	OK
2024-08-11 18:06:43	Android Permission Mapping Completed	OK
2024-08-11 18:06:48	Finished Code Analysis, Email and URL Extraction	OK
2024-08-11 18:06:48	Extracting String data from APK	OK
2024-08-11 18:06:51	Extracting String data from SO	OK
2024-08-11 18:06:51	Extracting String data from Code	OK
2024-08-11 18:06:52	Extracting String values and entropies from Code	OK
2024-08-11 18:06:57	Performing Malware check on extracted domains	OK
2024-08-11 18:07:03	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.