ANDROID STATIC ANALYSIS REPORT

Kidsy (2.7.66-google)

File Name:	Kidsy by FamiOn_merged.apk
Package Name:	global.kidsy.app
Scan Date:	Aug. 11, 2024, 2:15 p.m.

App Security Score:	51/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	i INFO	✓ SECURE	HOTSPOT
2	32	3	2	3

FILE INFORMATION

File Name: Kidsy by FamiOn_merged.apk
Size: 26.35MB
MD5: c13765df0b178f203d98c30df4ee9063
SHA1: a9a739ba03b840f6c7351d57a7f5b8e85c88f410
SHA256: 55d65c8d89bffaca3c2ba24fea5368ede6ed2cd81ae9bd199a44399de498c11f

APP INFORMATION

App Name: Kidsy
Package Name: global.kidsy.app
Main Activity: org.findmykids.app.presentation.screens.launcher.LauncherActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 2.7.66-google
Android Version Code: 2007660

APP COMPONENTS

Activities: 31
Services: 24
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: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-06-13 09:39:15+00:00
Valid To: 2053-06-13 09:39:15+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x797153c759f589b2b9285f408fcdb55f2edfb6b7
Hash Algorithm: sha256
md5: 3658af64b28c24c98b0806111865c1f1
sha1: 3b91a77abae3da57e90cc8888a4d9e759d3f9831

sha256: 821ee039509d9efd30afca792951664a64f6c7efbf0b775572a915e8086a4a20
sha512: 6d76b68fcecdcacb217089123af45f9abc6e6ea994357c7cc384a07aa58a407d9255138f5449db0a3ef89cf753600a98de7cca07e7f42b13660a49c0af9ec45e
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 98edba732331187e95f25e0d18bd2e42651d2d67e5d12a89e54f718b3bef8c0c
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_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.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".

PERMISSION	STATUS	INFO	DESCRIPTION
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.
global.kidsy.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

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.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8</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.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator check
network operator name check
ro.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.LauncherActivity	Schemes: fmk://, gmd://, https://, Hosts: @string/deeplink_domain, @string/branded_deeplink_domain,
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.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
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.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
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	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.
21	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.

NO	ISSUE	SEVERITY	DESCRIPTION
22	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.
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/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/manager/d.java com/bumptech/glide/manager/e.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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				r.java com/crowdin/platform/realtimeupdate/RealTimeUpdateManager.java com/crowdin/platform/screenshot/ScreenshotService.java com/crowdin/platform/util/ExtensionsKt.java com/intercom/twig/Twig.java defpackage/a10.java defpackage/a11.java defpackage/a49.java defpackage/a8.java defpackage/ad3.java defpackage/aeb.java defpackage/afb.java defpackage/ap.java defpackage/ar4.java defpackage/b07.java defpackage/b7.java defpackage/bc7.java defpackage/bob.java defpackage/br7.java defpackage/bvb.java defpackage/c0b.java defpackage/c6.java defpackage/c79.java defpackage/ca8.java defpackage/cc9.java defpackage/ci9.java defpackage/cj9.java defpackage/cn8.java defpackage/d47.java defpackage/d89.java defpackage/dc1.java defpackage/dd0.java defpackage/do4.java defpackage/dr4.java defpackage/ds8.java defpackage/eg5.java defpackage/eha.java defpackage/eq5.java defpackage/esa.java defpackage/f0b.java defpackage/f83.java defpackage/fd0.java defpackage/fd8.java defpackage/fdb.java defpackage/fl6.java defpackage/fla.java defpackage/fm6.java defpackage/fma.java defpackage/fr2.java defpackage/fua.java defpackage/gbb.java defpackage/gd0.java defpackage/gg5.java defpackage/gn3.java defpackage/goa.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/gpb.java defpackage/gv8.java defpackage/h02.java defpackage/h7.java defpackage/h97.java defpackage/hd8.java defpackage/hr4.java defpackage/hs2.java defpackage/hx0.java defpackage/ia5.java defpackage/ii1.java defpackage/ii8.java defpackage/ii9.java defpackage/is8.java defpackage/iy4.java defpackage/j6.java defpackage/jc.java defpackage/jd3.java defpackage/jdb.java defpackage/jh3.java defpackage/jk9.java defpackage/js2.java defpackage/ju4.java defpackage/jv8.java defpackage/jvb.java defpackage/k41.java defpackage/kf5.java defpackage/kj3.java defpackage/kma.java defpackage/ks0.java defpackage/ku4.java defpackage/kz7.java defpackage/la3.java defpackage/lo1.java defpackage/loa.java defpackage/ltb.java defpackage/lua.java defpackage/lx4.java defpackage/m83.java defpackage/m85.java defpackage/mbb.java defpackage/mc3.java defpackage/mcb.java defpackage/mk9.java defpackage/mo.java defpackage/mo1.java defpackage/ms8.java defpackage/mw7.java defpackage/mx4.java defpackage/n33.java defpackage/n42.java defpackage/n66.java defpackage/nj1.java defpackage/nk4.java defpackage/nl9.java defpackage/o01.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/o22.java defpackage/o4b.java defpackage/o88.java defpackage/ob9.java defpackage/of1.java defpackage/oj1.java defpackage/ola.java defpackage/os8.java defpackage/ou4.java defpackage/p05.java defpackage/p23.java defpackage/pa2.java defpackage/pb.java defpackage/pga.java defpackage/pm4.java defpackage/pm9.java defpackage/pq7.java defpackage/pya.java defpackage/qa3.java defpackage/qb1.java defpackage/qd2.java defpackage/qd9.java defpackage/qk5.java defpackage/qu0.java defpackage/r51.java defpackage/r7.java defpackage/r93.java defpackage/rd7.java defpackage/rg9.java defpackage/rk6.java defpackage/rka.java defpackage/rp3.java defpackage/s83.java defpackage/s85.java defpackage/sg9.java defpackage/sha.java defpackage/shb.java defpackage/sk5.java defpackage/sk9.java defpackage/sm2.java defpackage/snb.java defpackage/spa.java defpackage/sqb.java defpackage/stb.java defpackage/su4.java defpackage/svb.java defpackage/sx.java defpackage/t20.java defpackage/t25.java defpackage/t4.java defpackage/t61.java defpackage/t83.java defpackage/t97.java defpackage/tb1.java defpackage/te7.java defpackage/tga.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/tk3.java defpackage/tm9.java defpackage/tp.java defpackage/tq2.java defpackage/txa.java defpackage/u39.java defpackage/u5.java defpackage/u58.java defpackage/ub7.java defpackage/udb.java defpackage/uf.java defpackage/uj9.java defpackage/ula.java defpackage/uo4.java defpackage/uoa.java defpackage/up9.java defpackage/uu.java defpackage/uub.java defpackage/v00.java defpackage/v60.java defpackage/v85.java defpackage/vcb.java defpackage/vja.java defpackage/vk2.java defpackage/vk3.java defpackage/vp1.java defpackage/vp5.java defpackage/vpa.java defpackage/vq7.java defpackage/vr7.java defpackage/vs9.java defpackage/vt0.java defpackage/vtb.java defpackage/vw8.java defpackage/vxa.java defpackage/w39.java defpackage/w73.java defpackage/w77.java defpackage/w9.java defpackage/wf1.java defpackage/wf2.java defpackage/wja.java defpackage/wl8.java defpackage/ws1.java defpackage/ws4.java defpackage/wz0.java defpackage/x85.java defpackage/x93.java defpackage/xj5.java defpackage/xj9.java defpackage/y5a.java defpackage/y93.java defpackage/ydb.java defpackage/yg4.java defpackage/yi9.java defpackage/yq7.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/yqb.java defpackage/yva.java defpackage/z60.java defpackage/z87.java defpackage/zb8.java defpackage/zc9.java defpackage/zh8.java defpackage/zn2.java defpackage/zo.java defpackage/zq8.java
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/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/b18.java defpackage/d49.java defpackage/ev.java defpackage/h00.java defpackage/i85.java defpackage/j36.java defpackage/jx5.java defpackage/kg1.java defpackage/nz.java defpackage/o87.java defpackage/qx1.java defpackage/va2.java defpackage/vy.java defpackage/wy4.java defpackage/xx5.java defpackage/y15.java defpackage/yk2.java
3	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/cc9.java defpackage/gl6.java defpackage/ki6.java defpackage/o4.java defpackage/pn3.java defpackage/rm4.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	defpackage/h90.java defpackage/jz8.java defpackage/k0a.java defpackage/lx5.java defpackage/ub6.java defpackage/x51.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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/bk2.java defpackage/f0b.java defpackage/jv5.java defpackage/jw7.java defpackage/kl2.java defpackage/m76.java defpackage/nz6.java defpackage/r7.java defpackage/uc6.java defpackage/un9.java defpackage/vq1.java defpackage/z2.java
6	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
7	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/k0a.java
8	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/bg1.java defpackage/hj7.java defpackage/m33.java defpackage/sb4.java defpackage/wf7.java
9	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	defpackage/jd3.java defpackage/qr.java defpackage/ro.java defpackage/zl5.java
10	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/ct0.java
11	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	defpackage/a96.java defpackage/gg5.java defpackage/rx9.java defpackage/te7.java defpackage/v58.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	defpackage/cy0.java defpackage/hvb.java defpackage/n0a.java defpackage/odb.java
13	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	defpackage/zc9.java
14	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	defpackage/meb.java
15	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/kj3.java defpackage/n0a.java defpackage/ti0.java

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: 103.235.47.188 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:** 104.18.23.19 **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:** 13.32.110.17 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
sdlsdk.s	ok	No Geolocation information available.
ya.ru	ok	**IP:** 5.255.255.242 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
.facebook.com	ok	No Geolocation information available.
www.baidu.com	ok	**IP:** 103.235.47.188 **Country:** Hong Kong **Region:** Hong Kong **City:** Hong Kong **Latitude:** 22.285521 **Longitude:** 114.157692 **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
developers.facebook.com	ok	**IP:** 31.13.84.8 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebase.google.com	ok	**IP:** 172.217.20.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
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.
schemas.android.com	ok	No Geolocation information available.
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
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.

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
issuetracker.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
developer.apple.com	ok	**IP:** 17.253.15.197 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **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
firebase-settings.crashlytics.com	ok	**IP:** 142.250.180.195 **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:** 3.165.206.74 **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:** 185.199.108.153 **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.
simpression.s	ok	No Geolocation information available.
distributions.crowdin.net	ok	**IP:** 3.165.206.20 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
github.com	ok	**IP:** 140.82.121.3 **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:** 142.251.39.78 **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
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

DOMAIN	STATUS	GEOLOCATION
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.

EMAILS

EMAIL	FILE
u0013android@android.com u0013android@android.com0	defpackage/bfb.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
"com.google.firebase.crashlytics.mapping_file_id" : "d170a60923d54e6e83ca7cda6b0d7d0a"
"cross_auth_email" : "Email"

POSSIBLE SECRETS
"cross_auth_email_not_translateable" : "E-mail"
"cross_auth_units_email_title" : "Email"
"google_api_key" : "AIzaSyA7X1Knze2Qo4b5Z8U-FT3Q9qN84woF808"
"google_crash_reporting_api_key" : "AIzaSyA7X1Knze2Qo4b5Z8U-FT3Q9qN84woF808"
"intercom_api_key" : "android_sdk-b0ef5c43427c5301aa4f5c20bfcf4ca09b831d18"
"pingo_first_session_terms_got_it" : "Continue"
"pingo_first_session_lets_go" : "البداية"
"pingo_first_session_role_child" : "لنفسي"
"pingo_first_session_role_parent" : "لطفلي"
"pingo_first_session_terms_got_it" : "استمرار"
"step_connection_description_for_child_user" : "لطفل"
"cross_auth_email" : "E-poçt"
"cross_auth_units_email_title" : "E-poçt"
"pingo_first_session_lets_go" : "Başlayın"
"cross_auth_email" : "Е-адреса"
"cross_auth_units_email_title" : "Е-адреса"
"pingo_first_session_lets_go" : "Почетак"
"pingo_first_session_terms_got_it" : "Настави"
"cross_auth_email" : "Почта"
"cross_auth_units_email_title" : "Почта"
"pingo_first_session_lets_go" : "Вперёд!"
"pingo_first_session_role_child" : "Мне"

POSSIBLE SECRETS
"pingo_first_session_terms_got_it" : "Продолжить"
"cross_auth_email" : "Имейл"
"cross_auth_units_email_title" : "Имейл"
"pingo_first_session_lets_go" : "Начало!"
"pingo_first_session_terms_got_it" : "Продължи"
"cross_auth_code_sent_title" : "□□□□□□□□"
"cross_auth_email" : "□□□□"
"cross_auth_set_email" : "□□□□□□"
"cross_auth_units_email_title" : "□□□□"
"first_session_pingo_achive_action" : "□□□□□□"
"first_session_pingo_dialog_choose_avatar_camera" : "□□□□"
"first_session_pingo_dialog_choose_avatar_gallery" : "□□□□□□"
"first_session_pingo_dialog_desc_1" : "□□□□□□□□□□□□□"
"first_session_pingo_dialog_desc_4" : "□□□□□□□□□□□□□□□□□□"
"first_session_pingo_dialog_desc_5" : "□□□□□□□□□□□□□□□"
"first_session_pingo_dialog_desc_daughter_with_name_4" : "□□□□□□□□□%s□□□□□□"
"first_session_pingo_dialog_desc_daughter_with_name_5" : "%s□□□□□□□□□□□□"
"first_session_pingo_dialog_desc_son_with_name_4" : "□□□□□□□□□%s□□□□□□"
"first_session_pingo_dialog_desc_son_with_name_5" : "%s□□□□□□□□□□□□"
"live_stopped_reason_secret" : "□□□□"
"pingo_first_session_accept_terms" : "□□□□□□□□□□□□□□□□□□□[terms_link]□□□□[/terms_link]□[policy_link]□□□□[/policy_link]"
"pingo_first_session_age_title" : "□□□□□"

POSSIBLE SECRETS
"pingo_first_session_call_parent_v2" : "□□□□□□□□□□□□□"
"pingo_first_session_lets_go" : "□□"
"pingo_first_session_lets_setup_your_phone" : "□□□□□□□□□□□□"
"pingo_first_session_role_child" : "□□"
"pingo_first_session_role_parent" : "□□□□□□"
"pingo_first_session_terms_got_it" : "□□"
"pingo_first_session_who_are_you" : "□□□□□□□□□□□□"
"step_connection_description_for_child_user" : "□□□□"
"step_connection_description_for_parent_user" : "□□□□"
"cross_auth_email" : "Email"
"cross_auth_units_email_title" : "Email"
"pingo_first_session_lets_go" : "Spustit!"
"pingo_first_session_terms_got_it" : "Pokračovat"
"cross_auth_email" : "E-mail"
"cross_auth_units_email_title" : "E-mail"
"pingo_first_session_lets_go" : "Start!"
"pingo_first_session_terms_got_it" : "Fortsæt"
"cross_auth_email" : "E-Mail-Adresse"
"cross_auth_units_email_title" : "E-Mail-Adresse"
"live_stopped_reason_secret" : "Privatgespräch"
"pingo_first_session_terms_got_it" : "Weiter"
"cross_auth_email" : "Email"

POSSIBLE SECRETS
"cross_auth_units_email_title" : "Email"
"pingo_first_session_lets_go" : "Έναρξη"
"pingo_first_session_terms_got_it" : "Συνέχεια"
"cross_auth_email" : "Email"
"cross_auth_units_email_title" : "Email"
"pingo_first_session_terms_got_it" : "Continue"
"cross_auth_email" : "Email"
"cross_auth_units_email_title" : "Email"
"pingo_first_session_terms_got_it" : "Continue"
"cross_auth_email" : "E-mail"
"cross_auth_units_email_title" : "E-mail"
"pingo_first_session_lets_go" : "¡Vamos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"

POSSIBLE SECRETS
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"

POSSIBLE SECRETS
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"pingo_first_session_lets_go" : "¡Comencemos!"
"pingo_first_session_terms_got_it" : "Continuar"
"cross_auth_email" : "E-post"
"cross_auth_units_email_title" : "E-post"
"live_stopped_reason_secret" : "Salajutt"

POSSIBLE SECRETS
"pingo_first_session_lets_go" : "Algus!"
"pingo_first_session_terms_got_it" : "Jätka"
"step_connection_description_for_child_user" : "Lapsele"
"step_connection_description_for_parent_user" : "Lapsevanemale"
"cross_auth_email" : "ایمیل"
"cross_auth_units_email_title" : "ایمیل"
"pingo_first_session_lets_go" : "شروع"
"pingo_first_session_terms_got_it" : "ادامه"
"cross_auth_email" : "Sähköposti"
"cross_auth_units_email_title" : "Sähköposti"
"live_stopped_reason_secret" : "Salaisuudet"
"pingo_first_session_lets_go" : "Aloitetaan!"
"pingo_first_session_role_child" : "Minulle"
"pingo_first_session_role_parent" : "Lapselleni"
"pingo_first_session_terms_got_it" : "Jatka"
"step_connection_description_for_child_user" : "Lapselle"
"step_connection_description_for_parent_user" : "Vanhemmalle"
"cross_auth_email" : "E-mail"
"cross_auth_units_email_title" : "E-mail"
"pingo_first_session_terms_got_it" : "Continuer"
"cross_auth_email" : "אימייל"
"cross_auth_units_email_title" : "אימייל"

POSSIBLE SECRETS
"pingo_first_session_lets_go" : "מתחילים!"
"pingo_first_session_role_child" : "בשבילי"
"pingo_first_session_terms_got_it" : "המשך"
"step_connection_description_for_child_user" : "לילד"
"step_connection_description_for_parent_user" : "להורה"
"cross_auth_email" : "■-■■■"
"cross_auth_units_email_title" : "■-■■■"
"pingo_first_session_lets_go" : "■■■■■■■"
"cross_auth_email" : "E-mail"
"cross_auth_units_email_title" : "E-mail"
"pingo_first_session_lets_go" : "Početak!"
"pingo_first_session_terms_got_it" : "Nastavak"
"cross_auth_email" : "Email"
"cross_auth_units_email_title" : "Email"
"first_session_pingo_dialog_choose_avatar_camera" : "Kamera"
"pingo_first_session_lets_go" : "Kezdet!"
"pingo_first_session_role_child" : "Nekem"
"pingo_first_session_terms_got_it" : "Tovább"
"step_connection_description_for_child_user" : "Gyereknek"
"step_connection_description_for_parent_user" : "szülőknek"
"cross_auth_email" : "Email"
"cross_auth_units_email_title" : "Email"

POSSIBLE SECRETS
"live_stopped_reason_secret" : "Rahasia"
"pingo_first_session_lets_go" : "Mulai"
"pingo_first_session_terms_got_it" : "Lanjutkan"
"cross_auth_email" : "Email"
"cross_auth_units_email_title" : "Email"
"live_stopped_reason_secret" : "Rahasia"
"pingo_first_session_lets_go" : "Mulai"
"pingo_first_session_terms_got_it" : "Lanjutkan"
"cross_auth_email" : "Email"
"cross_auth_units_email_title" : "Email"
"pingo_first_session_lets_go" : "Iniziamo!"
"pingo_first_session_terms_got_it" : "Continua"
"cross_auth_email" : "אימייל"
"cross_auth_units_email_title" : "אימייל"
"pingo_first_session_lets_go" : "מתחילים!"
"pingo_first_session_role_child" : "בשבילי"
"pingo_first_session_terms_got_it" : "המשך"
"step_connection_description_for_child_user" : "לילד"
"step_connection_description_for_parent_user" : "להורה"
"cross_auth_code_sent_title" : "□□□□E□□□□□□□"
"cross_auth_email" : "E□□□"
"cross_auth_set_email" : "E□□□□□□□"

POSSIBLE SECRETS
"cross_auth_units_email_title" : "E□□□"
"first_session_child_here" : "%s□□□□□□□"
"first_session_pingo_achive_action" : "□□□"
"first_session_pingo_dialog_choose_avatar_camera" : "□□□□□□"
"first_session_pingo_dialog_choose_avatar_gallery" : "□□□□□□□□□"
"first_session_pingo_dialog_desc_1" : "□□□□□□□□□□□□□□□□□"
"first_session_pingo_dialog_desc_4" : "□□□□□□□□□□□□□□□□□□□□□□"
"first_session_pingo_dialog_desc_5" : "□□□□□□□□□□□□□□□□"
"first_session_pingo_dialog_desc_daughter_with_name_4" : "□□□□□□□□□□□□□%s□□□□□□□"
"first_session_pingo_dialog_desc_daughter_with_name_5" : "%s□□□□□□□□□□□□□□"
"first_session_pingo_dialog_desc_son_with_name_4" : "□□□□□□□□□□□□□%s□□□□□□□"
"first_session_pingo_dialog_desc_son_with_name_5" : "%s□□□□□□□□□□□□□□"
"intercom_article_double_author" : "□□□□{author_first_name1}□{author_first_name2}"
"intercom_article_multiple_authors" : "□□□□{author_first_name1}□□{number_of_other_authors}□"
"intercom_article_single_author" : "□□□□{author_first_name}"
"live_stopped_reason_secret" : "□□□□"
"pingo_first_session_age_title" : "□□□□□□"
"pingo_first_session_call_parent_v2" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"pingo_first_session_lets_go" : "□□□□"
"pingo_first_session_lets_setup_your_phone" : "□□□□□□□□□□□□□□□□□□□"
"pingo_first_session_role_child" : "□□□□□"
"pingo_first_session_role_parent" : "□□□□□"

POSSIBLE SECRETS
"pingo_first_session_terms_got_it" : "□□□"
"pingo_first_session_who_are_you" : "□□□□□□□□□□□□□□□□"
"step_connection_description_for_child_user" : "□□□□□□□"
"step_connection_description_for_parent_user" : "□□□□□□"
"first_session_pingo_achive_action" : "Иә!"
"pingo_first_session_lets_go" : "Басталуы"
"pingo_first_session_terms_got_it" : "Жалғастыру"
"cross_auth_email" : "□□□"
"cross_auth_units_email_title" : "□□□"
"first_session_pingo_achive_action" : "□!"
"pingo_first_session_lets_go" : "□□"
"pingo_first_session_role_child" : "□"
"pingo_first_session_terms_got_it" : "□□"
"step_connection_description_for_child_user" : "□□□"
"step_connection_description_for_parent_user" : "□□□□"
"first_session_pingo_dialog_choose_avatar_camera" : "Fotografuokite"
"pingo_first_session_lets_go" : "Pradėti"
"pingo_first_session_terms_got_it" : "Tęsti"
"step_connection_description_for_child_user" : "Vaikui"
"step_connection_description_for_parent_user" : "Tėčiui/Mamai"
"cross_auth_email" : "E-pasts"
"cross_auth_units_email_title" : "E-pasts"

POSSIBLE SECRETS
"pingo_first_session_lets_go" : "Sākums"
"pingo_first_session_role_child" : "Man"
"pingo_first_session_terms_got_it" : "Turpināt"
"step_connection_description_for_child_user" : "Bērnam"
"step_connection_description_for_parent_user" : "Vecākam"
"cross_auth_email" : "E-post"
"cross_auth_units_email_title" : "E-post"
"pingo_first_session_lets_go" : "Start"
"pingo_first_session_terms_got_it" : "Fortsett"
"cross_auth_email" : "E-mail"
"cross_auth_units_email_title" : "E-mail"
"pingo_first_session_lets_go" : "Begin"
"pingo_first_session_terms_got_it" : "Doorgaan"
"cross_auth_email" : "Email"
"cross_auth_units_email_title" : "Email"
"pingo_first_session_lets_go" : "Zaczynajmy"
"pingo_first_session_terms_got_it" : "Kontynuuj"
"cross_auth_email" : "Email"
"cross_auth_units_email_title" : "Email"
"pingo_first_session_lets_go" : "Início"
"pingo_first_session_terms_got_it" : "Seguinte"
"cross_auth_email" : "Email"

POSSIBLE SECRETS
"cross_auth_units_email_title" : "Email"
"pingo_first_session_terms_got_it" : "Continuar"
"cross_auth_email" : "E-mail"
"cross_auth_units_email_title" : "E-mail"
"pingo_first_session_lets_go" : "Start"
"pingo_first_session_terms_got_it" : "Continuați"
"cross_auth_email" : "Почта"
"cross_auth_units_email_title" : "Почта"
"pingo_first_session_lets_go" : "Вперёд!"
"pingo_first_session_role_child" : "Мне"
"pingo_first_session_terms_got_it" : "Продолжить"
"cross_auth_email" : "Email"
"cross_auth_units_email_title" : "Email"
"pingo_first_session_lets_go" : "Štart"
"pingo_first_session_terms_got_it" : "Pokračovať"
"cross_auth_email" : "Email"
"cross_auth_units_email_title" : "Email"
"pingo_first_session_lets_go" : "Začni"
"pingo_first_session_role_child" : "Zame"
"pingo_first_session_terms_got_it" : "Nadaljuj"
"cross_auth_email" : "Email"
"cross_auth_units_email_title" : "Email"

POSSIBLE SECRETS
"pingo_first_session_lets_go" : "Fillo"
"pingo_first_session_terms_got_it" : "Vazhdo"
"cross_auth_email" : "Mejladress"
"cross_auth_units_email_title" : "Mejladress"
"pingo_first_session_lets_go" : "Starta"
"pingo_first_session_terms_got_it" : "Fortsätt"
"cross_auth_code_sent_title" : "■■■■■■■■■■■■■"
"cross_auth_email" : "■■■■"
"cross_auth_set_email" : "■■■■■■■■"
"cross_auth_units_email_title" : "■■■■"
"first_session_pingo_achive_action" : "■■■■■"
"first_session_pingo_dialog_choose_avatar_camera" : "■■■■■■"
"first_session_pingo_dialog_choose_avatar_gallery" : "■■■■■■■■■■■■■■■"
"first_session_pingo_dialog_desc_1" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"first_session_pingo_dialog_desc_5" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"pingo_first_session_age_title" : "■■■■■■■■■■■"
"pingo_first_session_call_parent_v2" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"pingo_first_session_lets_go" : "■■■"
"pingo_first_session_lets_setup_your_phone" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"pingo_first_session_role_child" : "■■■■■■■"
"pingo_first_session_role_parent" : "■■■■■■■■■■■■"
"pingo_first_session_terms_got_it" : "■■■■■■■■■■"

POSSIBLE SECRETS
"pingo_first_session_who_are_you" : "■■■■■■■■■■■■■■■■■■■■■■■"
"step_connection_description_for_child_user" : "■■■■■■■■■■"
"step_connection_description_for_parent_user" : "■■■■■■■■■■■■■■"
"cross_auth_email" : "E-posta"
"cross_auth_units_email_title" : "E-posta"
"first_session_pingo_achive_action" : "Evet!"
"pingo_first_session_terms_got_it" : "Devam"
"cross_auth_email" : "Email"
"cross_auth_units_email_title" : "Email"
"pingo_first_session_lets_go" : "Уперед!"
"pingo_first_session_terms_got_it" : "Далі"
"cross_auth_email" : "Email"
"cross_auth_units_email_title" : "Email"
"cross_auth_code_sent_title" : "□□□□□□□□"
"cross_auth_email" : "□□□□"
"cross_auth_set_email" : "□□□□□□"
"cross_auth_units_email_title" : "□□□□"
"first_session_pingo_achive_action" : "□□□□□□"
"first_session_pingo_dialog_choose_avatar_camera" : "□□□□"
"first_session_pingo_dialog_choose_avatar_gallery" : "□□□□□□"
"first_session_pingo_dialog_desc_1" : "□□□□□□□□□□□□□"
"first_session_pingo_dialog_desc_4" : "□□□□□□□□□□□□□□□□□□"

POSSIBLE SECRETS
"first_session_pingo_dialog_desc_5" : "□□□□□□□□□□□□□□□"
"first_session_pingo_dialog_desc_daughter_with_name_4" : "□□□□□□□□□%s□□□□□□"
"first_session_pingo_dialog_desc_daughter_with_name_5" : "%s□□□□□□□□□□□□"
"first_session_pingo_dialog_desc_son_with_name_4" : "□□□□□□□□□%s□□□□□□"
"first_session_pingo_dialog_desc_son_with_name_5" : "%s□□□□□□□□□□□□"
"live_stopped_reason_secret" : "□□□□□"
"pingo_first_session_accept_terms" : "□□□□□□□□□□□□□□□□□□□[terms_link]□□□□[/terms_link]□[policy_link]□□□□[/policy_link]"
"pingo_first_session_age_title" : "□□□□□"
"pingo_first_session_call_parent_v2" : "□□□□□□□□□□□□□□"
"pingo_first_session_lets_go" : "□□"
"pingo_first_session_lets_setup_your_phone" : "□□□□□□□□□□□□□"
"pingo_first_session_role_child" : "□□"
"pingo_first_session_role_parent" : "□□□□□□"
"pingo_first_session_terms_got_it" : "□□"
"pingo_first_session_who_are_you" : "□□□□□□□□□□□□□"
"step_connection_description_for_child_user" : "□□□□□"
"step_connection_description_for_parent_user" : "□□□□□"
"intercom_article_single_author" : "□□□{author_first_name}"
"cross_auth_code_sent_title" : "□□□□□□□□□"
"cross_auth_email" : "□□□□□"
"cross_auth_set_email" : "□□□□□□□"
"cross_auth_units_email_title" : "□□□□□"

POSSIBLE SECRETS
"first_session_pingo_achive_action" : "□□□□□□"
"first_session_pingo_dialog_choose_avatar_camera" : "□□□□"
"first_session_pingo_dialog_choose_avatar_gallery" : "□□□□□□"
"first_session_pingo_dialog_desc_1" : "□□□□□□□□□□□□□□"
"first_session_pingo_dialog_desc_4" : "□□□□□□□□□□□□□□□□□□□"
"first_session_pingo_dialog_desc_5" : "□□□□□□□□□□□□□□□□□"
"intercom_article_double_author" : "□□□{author_first_name1}□{author_first_name2}"
"intercom_article_single_author" : "□□□{author_first_name}"
"live_stopped_reason_secret" : "□□□□"
"pingo_first_session_accept_terms" : "□□□□□□□□□□□□□□□□□□□□□[terms_link]□□□□[/terms_link]□[policy_link]□□□□[/policy_link]"
"pingo_first_session_age_title" : "□□□□□"
"pingo_first_session_call_parent_v2" : "□□□□□□□□□□□□□"
"pingo_first_session_lets_go" : "□□"
"pingo_first_session_lets_setup_your_phone" : "□□□□□□□□□□□□□□"
"pingo_first_session_role_child" : "□□□"
"pingo_first_session_role_parent" : "□□□□□"
"pingo_first_session_terms_got_it" : "□□"
"pingo_first_session_who_are_you" : "□□□□□□□□□□□□"
"step_connection_description_for_child_user" : "□□□□"
"step_connection_description_for_parent_user" : "□□□□"
756a18d015469157deb45aebd697eebd
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901

POSSIBLE SECRETS
afa8e68cdece85976f8a5a23b7db7774
0485de78a473be2850e99f865c0d331f
cc2751449a350f668590264ed76692694a80308a
c56fb7d591ba6704df047fd98f535372fea00211
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
ae2044fb577e65ee8bb576ca48a2f06e
470fa2b4ae81cd56ecbcda9735803434cec591fa
5bae185a7c59e709594f0bab1df18a2f
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
128-c20968b22ed168a498a4bf28ebadc7e883bd4b8c2dba719cb4c661a2c15147f5
da742c954d1b019c0e8c3a7eb4e40ca2
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
7fc098e10615a9c6daacc3aae166daaf
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
1497fe6d3ff464258f448d2ac6ce035f
d9ea72d42a1d9dd96c2b97d7ceb62d23
9b8f518b086098de3d77736f9458a3d2f6f95a37
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
2008dffa-cb3d-4010-a561-8f0f52d6dcea
8a3c4b262d721acd49a4bf97d5213199c86fa2b9

POSSIBLE SECRETS
3393c4a68480652e21c10f0f28f529a4
5181942b9ebc31ce68dacb56c16fd79f
b9834b3d46890f94943f52ad737044f5
d3d0540467196ca8019ea490f662fdc1
1634ac8041e59a0eeb107dcc6e33bfa4

PLAYSTORE INFORMATION

Title: Kidsy by FamiOn

Score: 4.623853 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Social **Play Store URL:** global.kidsy.app

Developer Details: ANKO Solutions LLC, 9003950025182651389, Office 353-075, Schon Business Park, Dubai Investment Park First, Dubai, United Arab Emirates, None, support@kidsapps.pro,

Release Date: Jul 12, 2023 **Privacy Policy:** Privacy link

Description:

Kidsy is the ultimate partner app to FamiOn GPS Location Tracker, designed to ensure the well-being and security of your children. With its powerful features and intuitive interface, Kidsy empowers you with real-time insights into your child's whereabouts, giving you the peace of mind. - Install FamiOn GPS Location Tracker on your phone. - Register and Generate Code: Complete the registration process and get a code for Kidsy. - Install Kidsy on Your Child's Phone and follow the setup instructions. Enter the code generated earlier to establish the connection. Done! Stay Connected and enjoy real-time updates and advanced safety features to keep them secure. Key Features of FamiOn GPS Location Tracker and Kidsy: Real-time GPS Tracking: Keep track of your child's location in real-time on a detailed map. Stay informed about their movements and ensure their safety, whether they're at school, outdoors, or on a family trip. Sound Around: Listen in to your child's surroundings, stay connected and be aware of their immediate environment, providing an extra layer of security during outdoor activities or when they're away from home. Safe zones and notifications: Set up custom geofences for designated safe zones and receive instant notifications when your child enters or exits these areas. Create geofences for home, school, or any important location. Loud signal: Stay connected and send loud signal even when your child's device is on silent mode. SOS button: In emergencies, your child can easily activate the SOS Button within the app. Be there for them when they need you the most and ensure their safety with this vital feature. The app requires the following access: - to the camera and photos - for the child’s avatar - to contacts - for the choice of a phone number when setting up the GPS watch - to the microphone -to send voice messages in the chat - push notifications - for notifications about your child’s movements and new chat messages Pair FamiOn GPS Location Tracker with Kidsy on your child's device to establish a secure connection. Please remember that Kidsy requires the child's permission for installation. Note that continued use of GPS running in the background can significantly impact battery life. We recommend configuring the app settings for optimal battery usage. Explore our user agreement and privacy policy for more information. If you have any suggestions or questions about our app, please reach out to our dedicated support team or visit our website. Your feedback is valuable to us as we strive to continuously improve our services. - User Agreement - https://kidstracker.pro/docs/terms-of-use - Privacy Policy - https://kidstracker.pro/docs/privacy-policy

SCAN LOGS

Timestamp	Event	Error
2024-08-11 14:15:05	Generating Hashes	OK
2024-08-11 14:15:05	Extracting APK	OK

2024-08-11 14:15:05	Unzipping	OK
2024-08-11 14:15:05	Getting Hardcoded Certificates/Keystores	OK
2024-08-11 14:15:09	Parsing AndroidManifest.xml	OK
2024-08-11 14:15:09	Parsing APK with androguard	OK
2024-08-11 14:15:11	Extracting Manifest Data	OK
2024-08-11 14:15:11	Performing Static Analysis on: Kidsy (global.kidsy.app)	OK
2024-08-11 14:15:11	Fetching Details from Play Store: global.kidsy.app	OK
2024-08-11 14:15:12	Manifest Analysis Started	OK
2024-08-11 14:15:12	Reading Network Security config from network_security_config.xml	OK
2024-08-11 14:15:12	Parsing Network Security config	OK
2024-08-11 14:15:12	Checking for Malware Permissions	OK
2024-08-11 14:15:12	Fetching icon path	OK
2024-08-11 14:15:12	Library Binary Analysis Started	OK
2024-08-11 14:15:12	Reading Code Signing Certificate	OK

2024-08-11 14:15:12	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/c13765df0b178f203d98c30df4ee9063/c13765df0b178f203d98c30df4ee9063.apk'])
2024-08-11 14:15:12	Running APKiD 2.1.5	OK
2024-08-11 14:15:18	Detecting Trackers	OK
2024-08-11 14:15:24	Decompiling APK to Java with jadx	OK
2024-08-11 14:16:13	Converting DEX to Smali	OK
2024-08-11 14:16:13	Code Analysis Started on - java_source	OK
2024-08-11 14:17:25	Android SAST Completed	OK
2024-08-11 14:17:25	Android API Analysis Started	OK
2024-08-11 14:18:30	Android Permission Mapping Started	OK
2024-08-11 14:19:18	Android Permission Mapping Completed	OK
2024-08-11 14:19:25	Finished Code Analysis, Email and URL Extraction	OK
2024-08-11 14:19:25	Extracting String data from APK	OK
2024-08-11 14:19:28	Extracting String data from Code	OK
2024-08-11 14:19:28	Extracting String values and entropies from Code	OK

2024-08-11 14:19:32	Performing Malware check on extracted domains	OK
2024-08-11 14:19:37	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.