MOBSF

ANDROID STATIC ANALYSIS REPORT

Alli360 (2.17.0)

File Name:	base.apk
Package Name:	app.kids360.kid
Scan Date:	Aug. 10, 2024, 10:50 p.m.

App Security Score: 51/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	24	2	2	1

FILE INFORMATION

File Name: base.apk
Size: 17.83MB
MD5: 76bd65c0e441c091078be03c1b087b52
SHA1: 0877810d5747232aea29b97ba760c5d4cef77076
SHA256: a5eddb738ff9a03b5d1262123af3e4061e1d41a80f5d6970f4cac831d6f7a9d6

APP INFORMATION

App Name: Alli360
Package Name: app.kids360.kid
Main Activity: app.kids360.kid.ui.onboarding.OnboardingActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 2.17.0
Android Version Code: 1722863247

APP COMPONENTS

Activities: 27
Services: 23
Receivers: 27
Providers: 6
Exported Activities: 1
Exported Services: 2
Exported Receivers: 11
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=RU, ST=Perm, L=Perm, O=Kids 360, CN=Ponomarev Leonid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-11-16 12:49:26+00:00
Valid To: 2045-11-10 12:49:26+00:00
Issuer: C=RU, ST=Perm, L=Perm, O=Kids 360, CN=Ponomarev Leonid
Serial Number: 0xa1828d5
Hash Algorithm: sha256
md5: 7d374ac09e24c578fc59d2f8e4ace3e3
sha1: 913551509aa7a2e951938af2ea43f225e76341be

sha256: d01c7cbda022277dd3d3793502e1df6db281185017030bcb1a3f4291429424bf
sha512: 5203db6c43243009edd32c9470dd7df9d18c58afe594af363d622a46efd58ce5e2d36910555ec449524ce63c72e37cb186a28052a4579c223e1fb78035179ae9
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: e829407c6ecf6fcddd607024eda9ae23848c061792e64ede0562ab33b8523157
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.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.
com.huawei.systemmanager.permission.ACCESS_INTERFACE	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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_SPECIAL_USE	normal	enables special-use foreground services.	Allows a regular application to use Service.startForeground with the type "specialUse".
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
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.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
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.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.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.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
app.kids360.kid.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	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 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dx</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</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
app.kids360.kid.ui.onboarding.OnboardingActivity	Schemes: https://, Hosts: deeplink.kids360.app, kids360kid.page.link, af-alli360.kids360.app, Path Prefixes: /kid,

ACTIVITY	INTENT
app.kids360.kid.ui.main.MainActivity	Schemes: https://, Hosts: deeplink.kids360.app, Paths: /kid/deep/main/tasksv2, Path Prefixes: /kid/deep/main/tasksv2/,

NETWORK SECURITY

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: **1** | WARNING: **14** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Activity (app.kids360.kid.ui.main.MainActivity) 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.
3	Broadcast Receiver (app.kids360.usages.read.ShutdownRegistrator) 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
4	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.
5	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.
6	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.
7	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.
8	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.
9	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.
10	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.
11	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.

NO	ISSUE	SEVERITY	DESCRIPTION
12	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.
13	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.
14	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.
15	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: **1** | WARNING: **8** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	bi/a.java c4/p1.java com/appsflyer/internal/AFb1gSDK.java com/appsflyer/internal/AFc1iSDK.java com/esotericsoftware/kryo/util/ObjectMap.java e4/q.java nj/d.java nj/h.java t9/s.java v8/p1.java w9/b.java zi/z.java
				a2/n0.java aa/k.java af/b.java af/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				af/j.java af/k.java af/m.java app/kids360/core/analytics/OwnAnalytics.java app/kids360/core/logger/LogcatPlugin.java app/kids360/core/mechanics/experiments/BaseExperiment.java app/kids360/core/mechanics/faq/FAQWebActivity.java app/kids360/core/mechanics/setup/Autostart.java app/kids360/kid/mechanics/accessibility/LimitWatcherExtKt$limited$1.java app/kids360/usages/misc/Logger.java app/kids360/usages/read/ShutdownRegistrator.java c6/k0.java cb/b.java cf/b.java cf/c.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/esotericsoftware/kryo/Kryo.java com/esotericsoftware/kryo/serializers/VersionFieldSerializer.java com/esotericsoftware/kryo/util/DefaultClassResolver.java com/esotericsoftware/kryo/util/Util.java com/esotericsoftware/minlog/Log.java com/huawei/agconnect/core/provider/AGConnectInitializeProvider.java com/intercom/twig/Twig.java d3/d.java db/f.java db/o.java db/p.java ed/f.java ed/o.java f6/a.java fe/b.java g8/f.java ge/c.java h6/h.java hd/g.java hl/a.java i6/a.java io/paperdb/DbStoragePlainFile.java j2/d.java j4/d.java k4/g.java k6/b.java kj/e.java l2/l.java l2/o.java l6/m0.java
2	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	

NO	ISSUE	SEVERITY	STANDARDS	FILES
				lb/p.java lb/q.java lb/r.java m2/f.java nc/d.java o1/m0.java o2/a.java o2/c.java o2/d.java o2/f.java o3/b.java oc/b.java p8/a.java pe/b0.java pe/d0.java pe/f0.java pe/g.java pe/k.java pe/x.java q3/a.java qc/g.java qe/a.java re/c.java re/f.java rk/c.java sa/a.java tb/a.java u2/d.java u5/b.java u5/n.java ub/a.java ud/g.java v0/g.java v0/w.java v3/a.java va/a.java w2/x.java wa/f0.java xb/h.java xc/i.java y3/n.java y5/a.java ya/a.java ya/b0.java ya/b1.java ya/c.java ya/e0.java ya/h1.java ya/l1.java ya/u0.java ya/x0.java ya/y0.java ya/z0.java ye/d.java yi/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	app/kids360/core/Const.java app/kids360/core/analytics/OwnAnalytics.java app/kids360/core/elk/ElkEventLogger.java app/kids360/core/platform/messaging/Message.java app/kids360/core/platform/messaging/WebSocketEnabledReporter.java app/kids360/core/repositories/AuthRepo.java app/kids360/core/repositories/UuidRepo.java app/kids360/core/repositories/remoteconfig/RemoteConfigRepo.java app/kids360/core/repositories/store/PoliciesRepo.java app/kids360/core/repositories/store/UsagesAppRepo.java app/kids360/core/repositories/store/UsagesDailyRepo.java app/kids360/core/utils/SharingBroadcastReceiver.java app/kids360/kid/mechanics/PinCodeHelper.java app/kids360/kid/mechanics/accessibility/ShortcutDetectorInteractor.java app/kids360/kid/mechanics/changeTimeDetector/TimeChangeDetectorInteractor.java app/kids360/kid/mechanics/demo/DemoInteractor.java app/kids360/kid/mechanics/experiments/GeoKidExperiment.java app/kids360/kid/mechanics/geo/GeoKidInteractor.java app/kids360/kid/mechanics/guards/GuardAnalyticsFacade.java app/kids360/kid/mechanics/iconupload/AppsIconUploader.java app/kids360/kid/mechanics/interestingFacts/InterestingFactInteractor.java app/kids360/kid/mechanics/logicLike/domain/LogicLikeKidInteractor.java app/kids360/kid/mechanics/onboarding/FirstSessionV2Interactor.java app/kids360/kid/mechanics/setup/A11yServiceShutdownReporter.java app/kids360/kid/mechanics/usages/DeleteTodayUsageDetector.java app/kids360/kid/mechanics/usages/UsageUploaderInteractor.java app/kids360/kid/ui/home/HomeViewModel.java app/kids360/kid/ui/home/HomeWithStatsFragment.java app/kids360/kid/ui/onboarding/OnboardingFlowViewModel.java app/kids360/kid/ui/onboarding/OnboardingPreferences.java app/kids360/kid/ui/onboarding/ageRequest/KidAgeInteractor.java app/kids360/kid/ui/onboarding/geo/PhysicalActivityOnboardingFragment.java app/kids360/kid/ui/onboarding/hint/HintService.java app/kids360/kid/ui/onboarding/name/ChildUuidNameAvatarInteractor.java bg/a.java kd/b.java ld/e.java ld/w.java s7/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t6/d.java t6/e.java vi/t0.java z1/h.java z1/s0.java z3/a.java
4	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	af/k.java
5	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	af/k.java fe/b.java
6	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	fe/c.java gg/k6.java l7/r0.java
7	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	app/kids360/core/mechanics/faq/FAQWebActivity.java app/kids360/kid/mechanics/logicLike/presentation/webView/LogicLikeWebViewImpl.java
8	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	tk/b.java
9	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	app/kids360/core/platform/ContextExtKt.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	xc/v.java
11	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	jj/c.java jj/d.java jj/i.java jj/j.java
12	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	app/kids360/core/platform/StringExtKt.java
13	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	z9/b.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/24	android.permission.SYSTEM_ALERT_WINDOW, android.permission.INTERNET, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.VIBRATE, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.READ_PHONE_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	9/45	android.permission.FOREGROUND_SERVICE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.ACTIVITY_RECOGNITION, android.permission.PACKAGE_USAGE_STATS, com.google.android.gms.permission.ACTIVITY_RECOGNITION, android.permission.CHANGE_WIFI_STATE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
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

DOMAIN	STATUS	GEOLOCATION
play.google	ok	**IP:** 216.239.32.29 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sadrevenue.s	ok	No Geolocation information available.
sdlsdk.s	ok	No Geolocation information available.
api.prod.findmykids.app	ok	**IP:** 116.202.117.176 **Country:** Germany **Region:** Sachsen **City:** Falkenstein **Latitude:** 50.477879 **Longitude:** 12.371290 **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
www.google.com	ok	**IP:** 142.251.37.4 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
kids-360-parental.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
ns.adobe.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
sapp.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.
wss.findmykids.org	ok	**IP:** 167.235.81.131 **Country:** Germany **Region:** Bayern **City:** Gunzenhausen **Latitude:** 48.323330 **Longitude:** 11.601220 **View:** Google Map
sgcdsdk.s	ok	No Geolocation information available.
www.youtube.com	ok	**IP:** 142.251.37.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
elk.kids360.app	ok	**IP:** 178.154.227.1 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
scdn-stestsettings.s	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.
sconversions.s	ok	No Geolocation information available.
issuetracker.google.com	ok	**IP:** 142.251.37.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.apple.com	ok	**IP:** 17.253.73.205 **Country:** Germany **Region:** Berlin **City:** Berlin **Latitude:** 52.524368 **Longitude:** 13.410530 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 142.251.36.227 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
helpcenter.kids360.app	ok	**IP:** 178.154.231.28 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
aomedia.org	ok	**IP:** 185.199.109.153 **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.
dashif.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
play.google.com	ok	**IP:** 142.251.36.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
kids360.onelink.me	ok	**IP:** 13.32.110.3 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
deeplink.kids360.app	ok	**IP:** 178.154.231.28 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
logiclike.com	ok	**IP:** 144.76.190.31 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
sars.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
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
worldtimeapi.org	ok	**IP:** 213.188.196.246 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
developer.android.com	ok	**IP:** 172.217.16.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
kids360.app	ok	**IP:** 178.154.225.26 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
kids360kid.page.link	ok	**IP:** 142.251.36.193 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
logiclike.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
websocket-manager.kids360.app	ok	**IP:** 178.154.231.28 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
sinapps.s	ok	No Geolocation information available.

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://kids-360-parental.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
support@kids360.app	Android String Resource

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
Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://kids-360-parental.firebaseio.com"
"google_api_key" : "AIzaSyBPhqxZ89y2bDp0cnJ_SRBjIWrTT-vuUF4"
"google_crash_reporting_api_key" : "AIzaSyBPhqxZ89y2bDp0cnJ_SRBjIWrTT-vuUF4"
"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}"
"intercom_article_single_author" : "□□□{author_first_name}"
"intercom_article_double_author" : "□□□{author_first_name1}□{author_first_name2}"
"intercom_article_single_author" : "□□□{author_first_name}"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
3be094134acebe34c36e6816b0b0bdbc
487914b203b2f98fccba43354c8a6842

POSSIBLE SECRETS
470fa2b4ae81cd56ecbcda9735803434cec591fa
ae2044fb577e65ee8bb576ca48a2f06e
5c725da8dd55f8c8c8aa5f46159b1e4f
5abf736af0deb16fa07301cb99e10d16
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
b75577c96513ab2b3ef7ded18a2f0cf9
128-c20968b22ed168a498a4bf28ebadc7e883bd4b8c2dba719cb4c661a2c15147f5
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
17520d139b26a789b1aefd09cf619033
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
e11bf873f6121328882f2b346daba386
9a04f079-9840-4286-ab92-e65be0885f95
e2719d58-a985-b3c9-781a-b030af78d30e
566e3549904594cfc9dd2f45057b5ac5
5181942b9ebc31ce68dacb56c16fd79f
183f065fcccfc7c869823cd02c1a83cd
c3096904ceec43e255c6377f39a98090
37c21b7602a9559d475e808ef7abba84
8be46c1573e3186e3921baa694ce0fe3
e6c56e937ff46fd1b27376a92e0edef5

POSSIBLE SECRETS
c3de0c6ed63f95b0fb7274d6d08c0d91
babf943b8fa1846923c692445e518b96
676c7c7dddfd5985317ff4d7d77f1d1e

PLAYSTORE INFORMATION

Title: Alli360 by Kids360

Score: 4.5346537 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Parenting **Play Store URL:** app.kids360.kid

Developer Details: ANKO Solutions LLC, 9003950025182651389, Office 353-075, Schon Business Park, Dubai Investment Park First, Dubai, United Arab Emirates, https://kids360.app/, info@kids360.app,

Release Date: Dec 10, 2020 **Privacy Policy:** Privacy link

Description:

Alli360 — is a service that helps parents to set time limits for children in entertainment applications and games The Alli360 app complements the “Kids360 for parents” app and must be installed on the device the teen is using This app provides you with the following options: Time limit - set a time limit for specific applications and games your teens uses Schedule - set schedules for school time and rest in the evening: games, social networks, and entertainment apps will not be available during the specified time List of applications - select applications you want to limit or block completely Time spent - see how much time your teen spends on their smartphone and identify their most used applications Always keep in touch - applications for calls, messages, taxis, and other non-entertainment applications will always be available and you will always be able to contact your school student. The “Kids360” app is designed for family safety and parental control. Thanks to the application tracker, you will always know how much time teen is spending on their smartphone. The app cannot be installed on the cell phone without your child’s knowledge, its use is available only with the explicit consent. Personal data is stored in strict accordance with legislation and GDPR policies. How to start using the "Kids360" app: 1. Install the “Kids360 for parents” app on your mobile device; 2. Install the “Kids360” app on your teen's phone and enter the link code with the parental device; 3. Allow monitoring of your teenager's smartphone in the app. In case of technical problems, you can always contact the 24-hour support service in the app or via the following email support@kids360.app You can monitor your time on the smartphone for free after connecting second device. Time management functions in applications are available during the trial period and by purchasing a subscription. The app asks for the following permissions: 1. Display over other apps - to block applications when time limit rules occur 2. Accessibility services - to limit time at the smartphone screen 3. Usage access - to collect statistics about the application uptime 4. Autostart - for constant operation of the application tracker on the device 5. Device admin apps - to protect against unauthorized deletion.

SCAN LOGS

Timestamp	Event	Error
2024-08-10 22:50:37	Generating Hashes	OK
2024-08-10 22:50:37	Extracting APK	OK
2024-08-10 22:50:37	Unzipping	OK

2024-08-10 22:50:37	Getting Hardcoded Certificates/Keystores	OK
2024-08-10 22:50:40	Parsing AndroidManifest.xml	OK
2024-08-10 22:50:40	Parsing APK with androguard	OK
2024-08-10 22:50:41	Extracting Manifest Data	OK
2024-08-10 22:50:41	Performing Static Analysis on: Alli360 (app.kids360.kid)	OK
2024-08-10 22:50:41	Fetching Details from Play Store: app.kids360.kid	OK
2024-08-10 22:50:41	Manifest Analysis Started	OK
2024-08-10 22:50:42	Checking for Malware Permissions	OK
2024-08-10 22:50:42	Fetching icon path	OK
2024-08-10 22:50:42	Library Binary Analysis Started	OK
2024-08-10 22:50:42	Reading Code Signing Certificate	OK
2024-08-10 22:50:42	Running APKiD 2.1.5	OK
2024-08-10 22:50:45	Detecting Trackers	OK
2024-08-10 22:50:48	Decompiling APK to Java with jadx	OK
2024-08-10 22:51:16	Converting DEX to Smali	OK

2024-08-10 22:51:16	Code Analysis Started on - java_source	OK
2024-08-10 22:51:58	Android SAST Completed	OK
2024-08-10 22:51:58	Android API Analysis Started	OK
2024-08-10 22:52:28	Android Permission Mapping Started	OK
2024-08-10 22:53:16	Android Permission Mapping Completed	OK
2024-08-10 22:53:19	Finished Code Analysis, Email and URL Extraction	OK
2024-08-10 22:53:19	Extracting String data from APK	OK
2024-08-10 22:53:20	Extracting String data from Code	OK
2024-08-10 22:53:20	Extracting String values and entropies from Code	OK
2024-08-10 22:53:23	Performing Malware check on extracted domains	OK
2024-08-10 22:53:26	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.