ANDROID STATIC ANALYSIS REPORT

Kids Place (3.9.40)

File Name:	Kids Place Parental Control_merged.apk
Package Name:	com.kiddoware.kidsplace
Scan Date:	Aug. 11, 2024, 1:02 p.m.

App Security Score:	48/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	38	1	2	2

FILE INFORMATION

File Name: Kids Place Parental Control_merged.apk

Size: 16.62MB

MD5: 514efd10c9b163e2fa50e9d294bffb3a

SHA1: 0547ae63b654f432d9b91250a61f9db6cf600c29

SHA256: f76331eadf948c734c0f11d6aecb6742d7f09c524a57a9414faad85b9cad58e8

APP INFORMATION

App Name: Kids Place

Package Name: com.kiddoware.kidsplace

Main Activity: com.kiddoware.kidsplace.LaunchActivity

Target SDK: 33

Min SDK: 21

Max SDK:

Android Version Name: 3.9.40

Android Version Code: 890

APP COMPONENTS

Activities: 83

Services: 34

Receivers: 24

Providers: 11

Exported Activities: 12

Exported Services: 9

Exported Receivers: 6

Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Paresh Joshi
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-03-13 00:39:29+00:00
Valid To: 2038-07-29 00:39:29+00:00
Issuer: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Paresh Joshi
Serial Number: 0x4d7c1241
Hash Algorithm: sha1
md5: 9f988ab6361891e021e18ee8f4a6ff31
sha1: 4640a9d09e3b97c3e2f48ba1acf1d8146ab5508d
```

sha256: f938caf000ba3d6d939891b5dc0364de15ca960934da9b22430da4801a038dbd
sha512: 1215da744fe40034693dff29203be26a0a7be5907b1890814258e7b03f14860c74a66b65e713f79995edd50f2e31553b09a94e84fb601349e20770b2227936cd
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: bc5e16ab299e51b84a66614398048385c74d1e6b0866ed2a376b27c09b6988ed
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.kiddoware.kidsvideoplayer.kidsvideoplayerprovider.READ	unknown	Unknown permission	Unknown permission from android reference
com.kiddoware.kidsvideoplayer.kidsvideoplayerprovider.READ_WRITE	unknown	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.KILL_BACKGROUND_PROCESSES	normal	kill background processes	Allows an application to kill background processes of other applications, even if memory is not low.
android.permission.RESTART_PACKAGES	normal	kill background processes	Allows an application to kill background processes of other applications, even if memory is not low.
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.SET_WALLPAPER	normal	set wallpaper	Allows the application to set the system wallpaper.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
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.SYSTEM_OVERLAY_WINDOW	unknown	Unknown permission	Unknown permission from android reference
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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.kiddoware.kidsplace.KPService.permission.Access	unknown	Unknown permission	Unknown permission from android reference
com.kiddoware.kidsplace.permission.CURRENT_RUNNING_APP	unknown	Unknown permission	Unknown permission from android reference
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.EXPAND_STATUS_BAR	normal	expand/collapse status bar	Allows application to expand or collapse the status bar.
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.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator 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>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.kiddoware.kidsplace.activities.WebViewActivity	Schemes: kiddoware://, Hosts: kidsplace,
com.kiddoware.kidsplace.activities.ParseDeepLinkActivity	Schemes: com.kiddoware.kidsplace://, https://, Hosts: deeplink, *.kiddoware.com,
com.facebook.CustomTabActivity	Schemes: @string/facebook_login_protocol_scheme://,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.

CERTIFICATE ANALYSIS

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

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

HIGH: **3** | WARNING: **27** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	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	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	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.
4	Content Provider (com.kiddoware.kidsplace.providers.AuthenticationProvider) is Protected by a permission. Permission: com.kiddoware.kidsplace.KPService.permission.Access protectionLevel: signature [android:exported=true]	info	A Content Provider is found to be exported, but is protected by permission.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Content Provider (com.kiddoware.kidsplace.providers.AppDataProvider) is Protected by a permission. Permission: com.kiddoware.kidsplace.KPService.permission.Access protectionLevel: signature [android:exported=true]	info	A Content Provider is found to be exported, but is protected by permission.
6	Content Provider (com.kiddoware.kidsplace.providers.UserDataProvider) is Protected by a permission. Permission: com.kiddoware.kidsplace.KPService.permission.Access protectionLevel: signature [android:exported=true]	info	A Content Provider is found to be exported, but is protected by permission.
7	Content Provider (com.kiddoware.kidsplace.providers.CategoryDataProvider) is Protected by a permission. Permission: com.kiddoware.kidsplace.KPService.permission.Access protectionLevel: signature [android:exported=true]	info	A Content Provider is found to be exported, but is protected by permission.
8	Content Provider (com.kiddoware.kidsplace.providers.PreferenceDataProvider) is Protected by a permission. Permission: com.kiddoware.kidsplace.KPService.permission.Access protectionLevel: signature [android:exported=true]	info	A Content Provider is found to be exported, but is protected by permission.
9	Content Provider (com.kiddoware.kidsplace.providers.AppLaunchesProvider) is Protected by a permission. Permission: com.kiddoware.kidsplace.KPService.permission.Access protectionLevel: signature [android:exported=true]	info	A Content Provider is found to be exported, but is protected by permission.
10	Content Provider (com.kiddoware.kidsplace.scheduler.db.TimesContentProvider) is Protected by a permission. Permission: com.kiddoware.kidsplace.KPService.permission.Access protectionLevel: signature [android:exported=true]	info	A Content Provider is found to be exported, but is protected by permission.
11	Activity (com.kiddoware.kidsplace.LockActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Activity (com.kiddoware.kidsplace.LockActivityWithGrownUpMode) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Activity (com.kiddoware.kidsplace.activities.WebViewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
14	App Link assetlinks.json file not found [android:name=com.kiddoware.kidsplace.activities.ParseDeepLinkActivity] [android:host=https://kiddoware.com]	high	App Link asset verification URL (https://kiddoware.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
15	Activity (com.kiddoware.kidsplace.activities.ParseDeepLinkActivity) 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.
16	Broadcast Receiver (com.kiddoware.kidsplace.admin.KPDeviceAdminReceiver) 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.
17	Broadcast Receiver (com.kiddoware.kidsplace.AutoStartKpReceiver) 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.
18	Service (com.kiddoware.kidsplace.KidsPlaceService) is Protected by a permission. Permission: com.kiddoware.kidsplace.KPService.permission.Access protectionLevel: signature [android:exported=true]	info	A Service is found to be exported, but is protected by permission.
19	Service (com.kiddoware.kidsplace.KidsPlaceAccessibilityService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_ACCESSIBILITY_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.
20	Service (com.kiddoware.kidsplace.activities.RemoteLockIntentService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
21	Activity (com.kiddoware.kidsplace.activities.FirebaseWebViewActivity) 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.
22	Service (com.kiddoware.kidsplace.firebase.KPFirebaseMessagingService) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
23	Broadcast Receiver (com.kiddoware.kidsplace.remotecontrol.mdm.service.LocationReceiver) 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.
24	Service (com.kiddoware.kidsplace.remotecontrol.geofence.GeofenceIntentService) 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.
25	Service (com.kiddoware.kidsplace.remotecontrol.geofence.GeofenceTransitionsService) 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.
26	Broadcast Receiver (com.kiddoware.kidsplace.remotecontrol.SynchronizationReceiver) 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.
27	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.
28	Activity (com.facebook.CustomTabActivity) 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.
29	Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
30	Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
31	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
32	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.
33	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.
34	Activity (androidx.biometric.DeviceCredentialHandlerActivity) 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.
35	Service (com.evernote.android.job.gcm.PlatformGcmService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_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.
36	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) 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.
37	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
38	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
39	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	fb/a.java p9/l.java za/z.java
				a0/c.java a0/e.java a0/f.java a0/g.java a0/k.java a3/e.java a3/f.java a3/k.java a3/l.java a3/n.java a3/o.java a7/a.java b0/c.java b0/m.java b3/d.java b8/f.java c5/m1.java c6/a.java cd/a.java com/airbnb/lottie/LottieAnimationView.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/c.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/g.java com/bumptech/glide/load/engine/i.java com/bumptech/glide/load/engine/w.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/a0.java com/bumptech/glide/load/resource/bitmap/c.java com/bumptech/glide/load/resource/bitmap/d.java com/bumptech/glide/load/resource/bitmap/l.java com/bumptech/glide/load/resource/bitmap/m.java com/bumptech/glide/load/resource/bitmap/q.java com/bumptech/glide/load/resource/bitmap/x.java com/bumptech/glide/request/SingleRequest.java com/firebase/ui/auth/KickoffActivity.java com/firebase/ui/auth/ui/email/WelcomeBackPasswordPrompt.java com/firebase/ui/auth/ui/email/a.java com/firebase/ui/auth/ui/idp/AuthMethodPickerActivity.java com/firebase/ui/auth/ui/idp/WelcomeBackIdpPrompt.java com/firebase/ui/auth/ui/phone/PhoneActivity.java com/firebase/ui/auth/ui/phone/c.java com/firebase/ui/auth/util/signincontainer/SaveSmartLock.java com/firebase/ui/auth/util/signincontainer/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	com/firebase/ui/auth/util/signincontainer/b.java com/firebase/ui/auth/viewmodel/d.java com/kiddoware/kidsplace/KidsPlaceService.java com/kiddoware/kidsplace/StartupReceiver.java com/kiddoware/kidsplace/Utility.java com/kiddoware/kidsplace/activities/launcher/y.java com/kiddoware/kidsplace/activities/n0.java com/kiddoware/kidsplace/activities/onboarding/d2.java com/kiddoware/kidsplace/admin/KPDeviceAdminReceiver.java com/kiddoware/kidsplace/d.java com/kiddoware/kidsplace/events/KPEventsManager$store$1.java com/kiddoware/kidsplace/events/f.java com/kiddoware/kidsplace/f.java com/kiddoware/kidsplace/f1.java com/kiddoware/kidsplace/inapp/b0.java com/kiddoware/kidsplace/remotecontrol/KPRCSettingsActivity.java com/kiddoware/kidsplace/remotecontrol/SoundService.java com/kiddoware/kidsplace/remotecontrol/a0.java com/kiddoware/kidsplace/remotecontrol/c.java com/kiddoware/kidsplace/remotecontrol/geofence/GeofenceTransitionsService.java com/kiddoware/kidsplace/remotecontrol/i.java com/kiddoware/kidsplace/remotecontrol/mdm/activity/MDMOperationActivity.java com/kiddoware/kidsplace/remotecontrol/mdm/service/LocationReceiver.java com/kiddoware/kidsplace/remotecontrol/p0.java com/kiddoware/kidsplace/remotecontrol/r0.java com/kiddoware/kidsplace/remotecontrol/u0.java com/kiddoware/kidsplace/reporting/api/network/a.java com/kiddoware/kidsplace/reporting/d.java com/kiddoware/kidsplace/scheduler/usage_details/HelpDialogActivity.java com/kiddoware/kidsplace/view/CircularBackPendingImageView.java com/kiddoware/kidsplace/view/PendingImageView.java com/kiddoware/library/billing/d.java com/kiddoware/library/singlesignon/f.java d3/j.java d4/b.java d7/a.java dc/s.java f/b.java f1/b.java f3/b.java fb/a.java g0/d.java g0/i.java g1/k.java g6/b.java g7/h.java g8/j.java gd/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				h3/a.java h4/i.java h6/h.java h6/v.java h6/w.java hd/m.java hd/s.java i2/e.java j/g.java j1/b.java j9/o.java k/c.java k0/k.java k1/m0.java k4/a.java kc/a.java l2/d.java l2/e.java m5/i.java m5/n.java mc/c.java md/b.java n1/h.java n2/b.java n2/j.java n2/l.java nb/a.java nb/b.java nb/c.java nb/i.java o2/c.java o2/e.java ob/d.java oc/c.java p0/c.java p2/i.java p2/j.java p9/l.java pd/a.java q2/e.java q2/i.java qc/a.java r2/a.java rc/a.java rc/b.java s/c.java s2/c.java s2/d.java s2/f.java s2/s.java s2/t.java s7/d.java sc/a.java sc/f.java t0/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t7/b.java t8/b0.java t8/f0.java t8/g0.java t8/j0.java t8/l.java t8/n.java t8/o0.java t8/u.java t8/v.java t8/x.java t8/y.java u2/a.java u3/c.java u5/e.java u8/g.java u8/o.java v3/e.java v7/g.java vc/h.java w0/a.java w4/a.java w4/d.java wc/a.java x3/a.java x5/m0.java x8/f.java xa/l2.java y2/a.java y2/d.java y2/j.java yc/c.java z/c.java z/d.java z/i.java z0/a.java z5/b.java z5/b0.java z5/d.java z5/n0.java z5/s0.java z5/w.java z5/z.java zc/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	com/evernote/android/job/h.java com/kiddoware/kidsplace/KidsPlaceRepository.java com/kiddoware/kidsplace/d.java com/kiddoware/kidsplace/remotecontrol/c.java dd/r.java gc/a.java h1/a.java j9/p.java jc/b.java kc/a.java o4/m0.java o4/t0.java yc/a.java yc/c.java
4	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	a5/e.java com/kiddoware/kidsplace/KidsLauncher.java com/kiddoware/kidsplace/activities/manage/h.java com/kiddoware/kidsplace/model/Category.java ic/h.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/a0.java io/grpc/internal/q1.java io/grpc/okhttp/f.java m9/a.java ma/y.java nb/c.java o6/c.java oc/c.java qe/a.java qe/b.java re/a.java ud/e.java ud/h.java
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	hd/s.java rc/b.java xe/c.java
6	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	com/kiddoware/kidsplace/backup/e.java com/kiddoware/kidsplace/remotecontrol/p0.java dc/m.java gc/a.java yc/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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	b9/e.java bb/b.java com/bumptech/glide/load/engine/c.java com/bumptech/glide/load/engine/n.java com/bumptech/glide/load/engine/u.java com/kiddoware/kidsplace/tasks/data/c.java ga/a.java io/grpc/internal/d2.java ja/f.java m2/d.java
8	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	com/kiddoware/kidsplace/Utility.java com/kiddoware/kidsplace/firebase/model/Device.java tc/a.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	b8/v.java g8/w.java
10	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	com/kiddoware/kidsplace/activities/onboarding/d2.java
11	Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.	warning	CWE: CWE-200: Information Exposure OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/kiddoware/kidsplace/activities/onboarding/d2.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	14/24	android.permission.WAKE_LOCK, android.permission.WRITE_SETTINGS, android.permission.GET_TASKS, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.SET_WALLPAPER, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_PHONE_STATE, android.permission.READ_EXTERNAL_STORAGE

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	9/45	android.permission.CHANGE_NETWORK_STATE, android.permission.CHANGE_WIFI_STATE, android.permission.FOREGROUND_SERVICE, android.permission.PACKAGE_USAGE_STATS, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, com.google.android.gms.permission.AD_ID, android.permission.ACCESS_BACKGROUND_LOCATION, 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
www.amazon.com	ok	**IP:** 162.219.225.118 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.536282 **Longitude:** -122.310402 **View:** Google Map
qa.app.kiddoware.com	ok	**IP:** 54.175.22.109 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
m.facebook.com	ok	**IP:** 31.13.84.36 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.84.36 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
www.google.com	ok	**IP:** 142.250.180.196 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
accounts.google.com	ok	**IP:** 142.250.145.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
kiddoware.com	ok	**IP:** 52.26.248.67 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
licensing.kiddoware.com	ok	**IP:** 34.212.217.51 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebase.google.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
kidsplace.s3.us-west-2.amazonaws.com	ok	**IP:** 52.92.190.178 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.251.39.2 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
phone.firebase	ok	No Geolocation information available.
schemas.android.com	ok	No Geolocation information available.
app.kiddoware.com	ok	**IP:** 44.224.22.251 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
www.kiddoware.com	ok	**IP:** 52.26.248.67 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
twitter.com	ok	**IP:** 104.244.42.65 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
googlemobileadssdk.page.link	ok	**IP:** 142.251.208.161 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
plus.google.com	ok	**IP:** 142.251.208.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
console.firebase.google.com	ok	**IP:** 142.250.180.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
xmlpull.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
kidsplace.kiddoware.com	ok	**IP:** 54.148.41.244 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.251.39.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
kids-place.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
support.google.com	ok	**IP:** 142.251.39.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.180.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebasestorage.googleapis.com	ok	**IP:** 142.251.208.106 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

FIREBASE DATABASES

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

EMAILS

EMAIL	FILE
support@kiddoware.com	vc/h.java
support@kiddoware.com	com/kiddoware/kidsplace/Utility.java
support@kiddoware.com□ support@kiddoware.com ykingsmart1@gmail.com □□□□□support@kiddoware.com □□□□□support@kiddoware.com□□□□□□□ □□□□□support@kiddoware.com□□□□□□□ □□□□□support@kiddoware.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
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" : "7d076adb4fab4328abac8dad353a5cf0"
"firebase_database_url" : "https://kids-place.firebaseio.com"
"google_api_key" : "AIzaSyBkF5uneF0noSgMlu-nRGCloPM9tyM_NKQ"
"google_crash_reporting_api_key" : "AIzaSyBkF5uneF0noSgMlu-nRGCloPM9tyM_NKQ"
"password" : "Password"
"twitter_consumer_key" : "CHANGE-ME"
"twitter_consumer_secret" : "CHANGE-ME"
"password" : "Passwort"
"password" : "Contraseña"
"password" : "Password"
"com.google.firebase.crashlytics.mapping_file_id" : "c9dd8d6f51f4462c8f5d1527fb2c4405"
"firebase_database_url" : "https://kids-place.firebaseio.com"
"google_api_key" : "AIzaSyBkF5uneF0noSgMlu-nRGCloPM9tyM_NKQ"
"google_crash_reporting_api_key" : "AIzaSyBkF5uneF0noSgMlu-nRGCloPM9tyM_NKQ"
"bio_auth" : "□□□□"
"bio_auth_desc" : "□□□"
"bio_auth_note" : "□□"
"biometric_auth" : "□□□□"
"biometric_auth_desc" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"default_user_name" : "□□□□□□□□□"
"firebase_login_desc" : "□□□"

POSSIBLE SECRETS
"firebase_login_expired" : "□□□□□□□□□□□□□□□□"
"menu_manage_user" : "□□□□□□□"
"menu_select_user" : "□□□□□□□□□□□□"
"menu_switch_user" : "□□□□□□□□"
"startWithLastSelectedUser" : "□□□□□□□□□□"
"password" : "Senha"
"password" : "Пароль"
"bio_auth" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"biometric_auth" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"biometric_auth_desc" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"default_user_name" : "■■■■■■■■■■■■■"
"firebase_login_expired" : "■■■■■■■■■■■"
"menu_manage_user" : "■■■■■■■■■■■"
"menu_select_user" : "■■■■■■■■■■"
"menu_switch_user" : "■■■■■■■■■"
"startWithLastSelectedUser" : "■■■■■■■■■■■■■■■"
"default_user_name" : "□□□□□"
"menu_manage_user" : "□□□□"
"menu_select_user" : "□□□□□"
"menu_switch_user" : "□□□□"
"startWithLastSelectedUser" : "□□□□□□□"

POSSIBLE SECRETS
"bio_auth" : "□□□□"
"bio_auth_desc" : "□□□□□□□□□□□□□□□□□□□□“□□□□”"
"bio_auth_note" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"biometric_auth" : "□□□□"
"biometric_auth_desc" : "□□□□□□□□□PIN"
"default_user_name" : "□□□□"
"menu_manage_user" : "□□□□"
"menu_select_user" : "□□□□"
"menu_switch_user" : "□□□□"
"startWithLastSelectedUser" : "□□□□□□"
"bio_auth" : "□□□□"
"bio_auth_desc" : "□□□□□□□□□□□□□□□□□□□□“□□□□“"
"bio_auth_note" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"biometric_auth" : "□□□□"
"biometric_auth_desc" : "□□“□□“□□□□□□□"
"default_user_name" : "□□□□□"
"menu_manage_user" : "□□□□"
"menu_select_user" : "□□□□□"
"menu_switch_user" : "□□□□"
"startWithLastSelectedUser" : "□□□□□□□"
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

POSSIBLE SECRETS
115792089210356248762697446949407573530086143415290314195533631308867097853951
rfBYaobM06JIPnbukgoyOwsb7bCc9rvkUNfR4KOQWHU=
dJwO6Cl9MRqD0Gc5K3JTdZycyClQqkAPKU0XDLxQQPeGCWqiQha6f2rP1wtqtwx3
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
444CCCBE8B2141456C3F8C371A2691E7
JgNevmfyr8lZxnvZfq3r729JgtxbLk039SjEVr1jMI7eztR3nd0tOgO6sMz+FJz+
lomf+VO0Ecj7WivSbw6aVWdgbo/lmDysFNgyXwY+gTY=
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
Kjj/NWt5Xw530zWkhsqzO18XZPoLer8GCJYwlVW4Z2TDaLFXmLCWh2yD69kBis5q
dGQnAya6a12xEk9RZqxizYv1KQcB0awlyegaC3HNbmw=
JcyGK+UJP268FQFtTaGhQAzoKUodZulOKvzraNGT5p3xvR5cM9kMk5tDQLTCBUij
EggzVxU0lX/1UlHAeEGUyUm45SOmio09y9T4hm0PM9xyGW0Fa8XV6zB35QkAF1yq
470fa2b4ae81cd56ecbcda9735803434cec591fa
B3EEABB8EE11C2BE770B684D95219ECB
BmCZi3wg7cX26+HP9p5KWWgFeCy6CBwpe84PbqLu08A=
z60w6+pWlGB4RCxkD/LDTBZ25WofjghjXXagNVA9cCM=
rLNLoOjJQBnuvnCDgD+yaoADKoI2087E89SpHXw4yFg=
9iQ5YMaDdmXd2AE0qa10oJyqmGZHX7XNUzgm4wdKztIQI9jbAXaOTiv6toK0AOKU
YC+pJVOZY25wDvtlWBPChLSjLU0iUh44DqTcbsbdAncZlcvrsOhFkSGXkkm3Hf4Z

POSSIBLE SECRETS
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d0101040500308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010019d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
d91a5ba5f3d2253bcfefe8c9f85a1fc1
L+eAMQBxQYtni61+5W3ps9X1nzCZQ5WzyUUXMjOuRZ4=
5Y5rtCIQhjVwnkrBvzpTMg0rZuVvyD2oudHeojlpiyRPt3QF1dIwn8qKzMnR3WrD
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
JUzcgAa7QiZMDmYjeHwtF22qOBbojTFP/5L28xsdeCx9uYvsAo6FDNhapuA6bStH
UdRLZDfL4bVVU0VX3qg8hi1McU3FMuLhNf0tRNLophcguwloVZffIAQP6VRf+/uk
hs3/rpu0ZtoaPE+A6aRGA1SNmSKC7zzkLMT9t285eJ8=
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
myj1nOfly7SmCD8TPLBSkg5Eqhpr16G4wLW5wXHtMTM=
Gdhi15k7cHPLVK8ak2AW2U8wWjJccRmTSeAAE7zSYYmR363nmijtloZo3WMMU3lH
U55JZyt+fru+djXeCzNGPL143KELIHwp5RNEO07WiP4=
DZ4YQMGjiiG80De3h2RdExLJLCk1HXfUitSGB3xdLKjSzFe5jaVRnSWLaDfXmTZ6
7f6416df5e88f2bbbbc93a2748e012e37b25219c1008bae52ef7cc17e712a1b9
rCh66yJZbGwhYsjh3a4o4nMI5ui67q2Fs4U69kJBF3k=
JTvnHx65Egq/4novhqSS3bMw+oihCNz02Yz4pG4S+kE=

POSSIBLE SECRETS
VbWvt5u3iV1e6mTKIEv50y8+Z2ekDgVJovyXyxeSHYc=
FdWssDbNTznwvaSwEiy9othUceULqhXS0NiSaXeIdQIZaN4heVunXmsWFB1bgBsj
wPLuRKbAvZPAiJqPYNBqgvUCesMc3+VTtpgM018gMz5F9Lz38uNUBeCfwu8TSv2X
fBdzdgD1bofuaKTW6LUcH7mpQ3p8BVkg+3EYXR2IWu4=
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
9MUQl4bkTrG/hbkOaiPEQeZR+Q1g5nerIUIYlLLAX+szyWBOaKlwxYudXHeApTjq
THnQW94FsCDUSM+XeJNpgUTCgMolxy7rl1LeD10r6fuFhGDZDxfkCa3f3R02TTfn
S/SJ7YtODXxfB+6o9UyIgHiId71g3ksNaRMWqG3MsynbaW5fZJkURKKNBmxPvqKI
115792089210356248762697446949407573529996955224135760342422259061068512044369
rN4de9ttzTEp3+iQIPyTFLSG8iLr2YuUXdQWnliGMSg=
ZDqFJ0I5g5uVDR0fSRJqwb59d8cP3p3/RbyvkYRlQc0=
3bfeb57ab22790f61282581f653b821d
qfl1DhKUvYvonhmDhl2HtQbINO0xIIYvKgMRQgz52nQi898Sh8QDGcMkGv/U7x7x
686479766013060971498190079908139321726943530014330540939446345918554318339765539424505774633321719753296399637136332111386476861244038034037280892707005449
w0yuMX287JAuExKzMpRTJqrOhPVTMBo6RInylnboEYs=
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78

POSSIBLE SECRETS
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
RukHQ2QyoItYcCVOmbl/vMdZ4cajSx2BB5kPudfplwo=
c103703e120ae8cc73c9248622f3cd1e
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
azGRTaieBebLUCBtXxWiGC8ntdSjezuXnKrD7NOMrfVnrrLI+ziOvss+bqlk4xLN
a17x9Lt/WQTGhUJAM6t8VqFWsXteADIsbbHvy7b7aMM=
uXer3UA11jv0SZxM8rEYS7HzXCd8ucSITS/VghhemVPtPpwzWKxJYN2vUPP5dw9E
13swnHoz78V4UQSpBM2KHvpNNnXpuWx8GAjTYu5TVQw=
yXOhM6UEm+Qz/JUey2l1+qI404D+W2SeSSnUBSRl6qI=
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
ylslQbtrjnaBQeIQLiG5TQpHgACRff6HBxNL0ysPa0Q=
ocyv6C8QcbvM773uNIAZp2X4LXa0iaH/WiMOnB1xz18=
f+92zzsRq9nsZjabs/oaBlCH7RtiJvk62T7dPsPTbRg=
Jj1vyuWfy0iUak+iXdGffQYzyyVnoa3nOmSynhrPgns=
2VR7L/2srPLBbh3OPlGeS8Ru8uYXtYmourWjxCdZl0ZvDKChHNCuDLRy98nk4nFB
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186160697311231 9

POSSIBLE SECRETS
49f946663a8deb7054212b8adda248c6
0tQXY1xo2ukrM9W+s0u6j2Mh+vSCsclEF17Hl/ROszM=
TzSf4nrBofZD4sG4/0KqSG9VhwNKl95AgxoEIclkVIM=
XOTxexwsk5wzpmsanl+x8sPTZMmLepw+z7JZ/NtNU48=
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643

PLAYSTORE INFORMATION

Title: Kids Place Parental Control

Score: 4.13093 **Installs:** 5,000,000+ **Price:** 0 **Android Version Support:** **Category:** Entertainment **Play Store URL:** com.kiddoware.kidsplace

Developer Details: Kiddoware - Parental Control App Provider, 8669878528475317483, 1314 E. Calle De Arcos, Tempe, AZ, 85284 USA., https://kiddoware.com, support@kiddoware.com,

Release Date: Oct 16, 2011 **Privacy Policy:** Privacy link

Description:

Kids Place is one of the best Free Parental Control App: Trusted by Millions of Parents world wide! Kids Place Free Parental Controls App is a screen time limit & parental control app created for parents who want to control their children's activity & screen time control on phones & tablets. Kids Mode, Screen Time Control & Child Lock & parental control app features give parents a lot of flexibility on how to configure their phone/tablets to for screen time control, block ads & inappropriate content. Parental Controls App & Screen Time Control allows you to digital ground rules for your children while guiding them as they learn, play, & explore online. Child Security App - full-featured, free parental control app on Google Play to secure kids zone for a safe family. This kids mode app & screen time control app creates a special kid area for your child where parents can manage your kids' screen time, lock on samsung, pixel, realme, oppo, motorola, oneplus, lg & other android devices, set time limit on app usage, & website control. Use this kids mode app free to limit phone usage via child lock & screen time control. □CREATE A SAFE ENVIRONMENT FOR YOUR KID with Kids Space on their device You decide which app can be accessed by your children to secure kids in the safest & most convenient way. This versatile free parental control app enables the easiest & most efficient Kids Space, Kids zone, Child Lock & Screen Time controls. Have you set a limit on your kids' phone usage, but they still ask to use yours? ✓ You can launch the app in kids space / kids lock mode on your device when you hand it over to them or it can be installed directly on their phone. Do you want to limit access to certain apps, which you don't find suitable for their age? ✓ This screen time control & free parental control app allows you to select all apps they can use & restrict access to these apps only when you lend your phone Are you worried that your children can accidentally download paid apps or buy credits for a game? ✓ Activate blocking options for purchases from Google Play & don't allow new apps download while you let your kids play Want to disable internet access for your kids? ✓ Use Safe Browser plugin for internet safety for kids! ✓ Set a screen time control to limit the use of the phone or just some apps by children & control their screen time. ✓ Works seamlessly on Samsung, Huawei, Pixel, LG, OnePlus, Oppo, Vivo, Motorola and other Android devices along with google family link app Kids Place Parental Control App Free Features: ✓ Child Friendly Launcher with child lock and Kids Space ✓ Control what apps are visible and accessible by kids ✓ Block unapproved apps ✓ Create and Approve Tasks for Kids and offer Rewards for chores. Kids Place Parental Control App Premium Features: ✓ Create custom user profiles ✓ Set a daily timer for the phone or for single apps for screen time control. ✓ Change the name of the app & run it in the background ✓ Automatically restart it every time the phone is turned on ✓ Block app uninstall & protect your PIN Kids Place Premium is suitable when it is installed directly on your children's phones to create a safe kids space. ★This kids launcher application uses the Device Administrator permission. This is completely optional but is requested in case parents want to tamper proof the app for kids. ★This application uses Accessibility Service API permission. This is optional and is requested when user wants additional parental controls app security, specially to lock notification bar to prevent access to settings & uninstall by kids. Thanks to complementary products, which can be easily integrated with Kids Place, this free Parental Control app can also be extended to safe search web browsing & online video viewing. Keywords: Parental Control App, Screen Time Control, Child Lock, Kids Lock, Kids Mode, Kids Space, Family Time, Safe Kids Zone, Android Parental Control, Free Parental Control App

SCAN LOGS

Timestamp	Event	Error
2024-08-11 13:02:25	Generating Hashes	OK
2024-08-11 13:02:25	Extracting APK	OK
2024-08-11 13:02:25	Unzipping	OK
2024-08-11 13:02:25	Getting Hardcoded Certificates/Keystores	OK
2024-08-11 13:02:28	Parsing AndroidManifest.xml	OK
2024-08-11 13:02:28	Parsing APK with androguard	OK
2024-08-11 13:02:29	Extracting Manifest Data	OK
2024-08-11 13:02:29	Performing Static Analysis on: Kids Place (com.kiddoware.kidsplace)	OK
2024-08-11 13:02:29	Fetching Details from Play Store: com.kiddoware.kidsplace	OK
2024-08-11 13:02:30	Manifest Analysis Started	OK
2024-08-11 13:02:44	Reading Network Security config from network_security_config.xml	OK
2024-08-11 13:02:44	Parsing Network Security config	OK
2024-08-11 13:02:44	Checking for Malware Permissions	OK
2024-08-11 13:02:44	Fetching icon path	OK

2024-08-11 13:02:44	Library Binary Analysis Started	OK
2024-08-11 13:02:44	Reading Code Signing Certificate	OK
2024-08-11 13:02:44	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/514efd10c9b163e2fa50e9d294bffb3a/514efd10c9b163e2fa50e9d294bffb3a.apk'])
2024-08-11 13:02:44	Running APKiD 2.1.5	OK
2024-08-11 13:02:47	Detecting Trackers	OK
2024-08-11 13:02:49	Decompiling APK to Java with jadx	OK
2024-08-11 13:03:13	Converting DEX to Smali	OK
2024-08-11 13:03:13	Code Analysis Started on - java_source	OK
2024-08-11 13:03:38	Android SAST Completed	OK
2024-08-11 13:03:39	Android API Analysis Started	OK
2024-08-11 13:03:51	Android Permission Mapping Started	OK
2024-08-11 13:05:46	Android Permission Mapping Completed	OK
2024-08-11 13:05:47	Finished Code Analysis, Email and URL Extraction	OK
2024-08-11 13:05:47	Extracting String data from APK	OK

2024-08-11 13:05:47	Extracting String data from Code	OK
2024-08-11 13:05:47	Extracting String values and entropies from Code	OK
2024-08-11 13:05:50	Performing Malware check on extracted domains	OK
2024-08-11 13:05:53	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.