ANDROID STATIC ANALYSIS REPORT

FamilyTime Jr (3.14.6.ps)

File Name:	FamilyTime Jr_merged.apk
Package Name:	io.familytime.parentalcontrol
Scan Date:	Aug. 15, 2024, 11:42 p.m.

App Security Score:	52/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	30	2	2	1

FILE INFORMATION

File Name: FamilyTime Jr_merged.apk
Size: 17.54MB

MD5: cc69bc6bb14ebe2054f3f31fdb64719f
SHA1: a0c934767f748b3d476862d55cf6aaf9c9026d0a
SHA256: 8c2a5c3ad53437f3cf312d54e9e0e71c56275d553ae2da80e6aba3704339e9d1

ℹ APP INFORMATION

App Name: FamilyTime Jr
Package Name: io.familytime.parentalcontrol
Main Activity: io.familytime.parentalcontrol.activities.SplashActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 3.14.6.ps
Android Version Code: 3417

APP COMPONENTS

Activities: 31
Services: 19
Receivers: 23
Providers: 4
Exported Activities: 0
Exported Services: 5
Exported Receivers: 14
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: OU=Soracode, CN=Aziz Ahmed
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-05-22 12:17:18+00:00
Valid To: 2040-05-15 12:17:18+00:00
Issuer: OU=Soracode, CN=Aziz Ahmed
Serial Number: 0x8f80460
Hash Algorithm: sha256
md5: d50fb81d2e19b39ee5484977555c336f
sha1: bd5ba65447ac701d880d56aa187a4076e67e10a8
sha256: 90f809653683ccdb4e9130c70a267960d3c72337fe2788bf6575458029f2d61a
sha512: 888b8644d5d4e602fca44e1597210e1c63ad1403e6e00faec9295066648664b6cd6129d124434265785f0fd378db29889d434cd0120f8ff8fd48e86241d9f47c
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 422e215b7955d994e70f85550ee2bb146c4e00106e4cfa275e6c499d279331d1
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE_SYSTEM_EXEMPTED	normal	allows system-exempted types of foreground services.	Allows a regular application to use Service.startForeground with the type "systemExempted". Apps are allowed to use this type only in the use cases listed in ServiceInfo.FOREGROUND_SERVICE_TYPE_SYSTEM_EXEMPTED .
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.BROADCAST_CLOSE_SYSTEM_DIALOGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.INTERACT_ACROSS_USERS	unknown	Unknown permission	Unknown permission from android reference
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
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.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.BIND_NOTIFICATION_LISTENER_SERVICE	signature	required by NotificationListenerServices for system binding.	Must be required by an NotificationListenerService, to ensure that only the system can bind to it.
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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.EXPAND_STATUS_BAR	normal	expand/collapse status bar	Allows application to expand or collapse the status bar.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
android.permission.GET_PACKAGE_SIZE	normal	measure application storage space	Allows an application to find out the space used by any package.
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_SECURE_SETTINGS	SignatureOrSystem	modify secure system settings	Allows an application to modify the system's secure settings data. Not for use by common applications.
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.
io.familytime.parentalcontrol.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

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

FILE	DETAILS	
	FINDINGS	DETAILS
classes2.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check Build.TAGS check network operator name check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)

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: **21** | 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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Service (io.familytime.parentalcontrol.fcm.MyFirebaseMessagingService) 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.
4	Service (io.familytime.parentalcontrol.services.AccessibilityService) 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.
5	Service (io.familytime.parentalcontrol.services.AccessibilityService) 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.
6	Broadcast Receiver (io.familytime.parentalcontrol.featuresList.battery.BatteryStatusReceiver) 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 (io.familytime.parentalcontrol.featuresList.location.LocationUpdateReceiver) 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 (io.familytime.parentalcontrol.featuresList.location.LocationUpdatesBroadcastReceiver) 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 (io.familytime.parentalcontrol.receivers.DateTimeChangeReceiver) 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 (io.familytime.parentalcontrol.receivers.MyDeviceAdminReceiver) 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.
11	Broadcast Receiver (io.familytime.parentalcontrol.featuresList.installAppModule.receivers.AppInstallReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
12	Broadcast Receiver (io.familytime.parentalcontrol.featuresList.installAppModule.receivers.InstallAppsUploadReceiver) 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.
13	Broadcast Receiver (io.familytime.parentalcontrol.featuresList.smsmodule.reciever.SmsBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Broadcast Receiver (io.familytime.parentalcontrol.featuresList.contactWatchList.ContactsWatchlistReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
15	Broadcast Receiver (io.familytime.parentalcontrol.receivers.AppReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
16	Broadcast Receiver (io.familytime.parentalcontrol.featuresList.geofence.GeofenceBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
17	Service (io.familytime.parentalcontrol.featuresList.notificationLisner.NotificationService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_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.
18	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.
19	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.
20	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
21	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.
22	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

CODE ANALYSIS

HIGH: 0 | WARNING: 7 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a1/o.java a1/r.java a1/v0.java a3/d.java a7/c0.java a7/d0.java a7/g.java a7/j.java a7/v.java a7/z.java aa/a.java b3/w.java b7/a.java b9/a.java ba/c.java ba/e.java be/g.java c1/a.java c3/e.java c3/f0.java c3/j0.java c3/u.java c3/x.java c7/b.java c7/e.java ca/a.java com/airbnb/lottie/utils/d.java com/bumptech/glide/Glide.java com/bumptech/glide/gifdecoder/c.java com/bumptech/glide/gifdecoder/d.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/i.java com/bumptech/glide/load/data/mediastore/c.java com/bumptech/glide/load/data/mediastore/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/bitmap_recycle/f.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/cache/c.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/g.java com/bumptech/glide/load/engine/k.java com/bumptech/glide/load/engine/r.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/a.java com/bumptech/glide/load/model/g.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/bitmap/c.java com/bumptech/glide/load/resource/bitmap/d.java com/bumptech/glide/load/resource/bitmap/m.java com/bumptech/glide/load/resource/bitmap/q.java com/bumptech/glide/load/resource/gif/a.java com/bumptech/glide/load/resource/gif/d.java com/bumptech/glide/load/resource/gif/i.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/SingletonConnectivityReceiver.java com/bumptech/glide/manager/d.java com/bumptech/glide/manager/k.java com/bumptech/glide/manager/l.java com/bumptech/glide/manager/m.java com/bumptech/glide/module/c.java com/bumptech/glide/util/pool/FactoryPools.java com/hbb20/CountryCodePicker.java com/hbb20/a.java com/j256/ormlite/android/AndroidLogBackend.java com/j256/ormlite/android/apptools/OrmLiteConfigUtil.java com/j256/ormlite/logger/ConsoleLogBackend.java com/j256/ormlite/table/BaseSchemaUtils.java da/a.java de/blinkt/openvpn/core/OpenVPNService.java e2/d.java e9/h.java e9/o.java ea/a.java ea/b.java f1/e.java f2/d.java f2/h.java f6/b.java g0/a.java g1/a.java g2/b.java g6/c.java ga/a.java h3/b.java h7/b0.java h7/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	h7/z.java h9/d.java ha/a.java i1/b.java i3/e.java i3/n.java i3/o.java io/familytime/parentalcontrol/activities/CustomWebViewActivity.java io/familytime/parentalcontrol/activities/HomeActivity.java io/familytime/parentalcontrol/activities/LoginActivity.java io/familytime/parentalcontrol/activities/PassCodeProtectionScreen.java io/familytime/parentalcontrol/activities/PrivacyPolicyActivity.java io/familytime/parentalcontrol/activities/ResponseBackActivity.java io/familytime/parentalcontrol/activities/SplashActivity.java io/familytime/parentalcontrol/activities/UnLockScreenActivity.java io/familytime/parentalcontrol/bottosheets/PickMeBottomSheetFragment.java io/familytime/parentalcontrol/bottosheets/SOSBottomSheetFragment.java io/familytime/parentalcontrol/contacts/c.java io/familytime/parentalcontrol/database/db/DatabaseHelper.java io/familytime/parentalcontrol/database/db/a.java io/familytime/parentalcontrol/fcm/MyFirebaseMessagingService.java io/familytime/parentalcontrol/featuresList/appblocker/ui/BlockAppActivity.java io/familytime/parentalcontrol/featuresList/battery/BatteryStatusReceiver.java io/familytime/parentalcontrol/featuresList/callLogs/a.java io/familytime/parentalcontrol/featuresList/callLogs/c.java io/familytime/parentalcontrol/featuresList/contactWatchList/ContactsWatchlistReceiver.java io/familytime/parentalcontrol/featuresList/dailyLimit/model/ForegroundApp.java io/familytime/parentalcontrol/featuresList/geofence/GeofenceBroadcastReceiver.java io/familytime/parentalcontrol/featuresList/installAppModule/receivers/AppInstallReceiver.java io/familytime/parentalcontrol/featuresList/location/LocationUpdatesBroadcastReceiver.java io/familytime/parentalcontrol/featuresList/notificationLisner/NotificationService.java io/familytime/parentalcontrol/featuresList/smsmodule/reciever/SmsBroadcastReceiver.java io/familytime/parentalcontrol/fragments/home/AboutFragment.java io/familytime/parentalcontrol/fragments/home/HomeFragment.java io/familytime/parentalcontrol/fragments/home/PickMeFragment.java io/familytime/parentalcontrol/fragments/home/SOSFragment.java io/familytime/parentalcontrol/fragments/login/LoginFragment.java io/familytime/parentalcontrol/fragments/login/RegisterAddImageFragment.java io/familytime/parentalcontrol/fragments/login/SignupFragment.java io/familytime/parentalcontrol/fragments/permissions/EmergencyContactFragment.java io/familytime/parentalcontrol/fragments/permissions/InstallAppsPermissionFragment.java io/familytime/parentalcontrol/fragments/permissions/PermissionOverviewFragment.java io/familytime/parentalcontrol/fragments/permissions/VpnFragment.jav

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a io/familytime/parentalcontrol/receivers/AppReceiver.java io/familytime/parentalcontrol/retrofit/a.java io/familytime/parentalcontrol/services/AccessibilityService.java io/familytime/parentalcontrol/services/HeartBeatService.java io/familytime/parentalcontrol/utils/Utilities.java io/familytime/parentalcontrol/utils/a.java io/familytime/parentalcontrol/utils/b.java io/familytime/parentalcontrol/utils/c.java k4/c.java k9/a.java l3/b.java l4/b.java l5/a.java l9/a.java m1/a.java m2/j.java ma/c.java mc/d.java n9/a.java o1/k.java o6/c.java o9/b.java oa/a.java oa/h.java oa/k.java oa/q.java oa/u.java p2/a.java p8/p.java p9/c.java p9/d.java q/b.java q0/a.java q5/f.java q9/a.java q9/b.java ra/a.java s/j.java s/l.java s9/c.java sa/q.java sa/r.java t9/a.java ta/a0.java ta/c0.java ta/d0.java ta/i.java ta/j.java ta/k0.java ta/l.java ta/m.java ta/p0.java ta/r.java ta/u.java ta/y.java ta/z.java u/f.java u4/p.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				u4/p.java ua/b.java v/a.java v/c.java v/d.java v/e.java v1/a.java v9/a.java v9/b.java vc/c.java w0/c.java w0/e.java w1/a.java w1/d.java w2/a.java w2/d.java w3/a.java w9/c.java x3/a.java y0/b.java y1/a.java y6/a.java y6/e.java y9/a.java z2/d0.java z2/g.java z2/i0.java z2/l.java z2/m.java z2/n0.java z2/q.java z2/z.java z3/h.java z4/t.java z9/b.java z9/e.java z9/f.java z9/g.java
2	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	a1/d.java a1/f0.java a1/o.java com/j256/ormlite/android/AndroidCompiledStatement.java com/j256/ormlite/android/AndroidDatabaseConnection.java com/j256/ormlite/android/compat/ApiCompatibility.java com/j256/ormlite/android/compat/BasicApiCompatibility.java com/j256/ormlite/android/compat/JellyBeanApiCompatibility.java f1/d.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	io/familytime/parentalcontrol/retrofit/controler/a.java na/a.java uc/c.java uc/d.java uc/i.java uc/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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/b.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/c.java com/bumptech/glide/load/engine/p.java com/bumptech/glide/manager/RequestManagerRetriever.java f6/b.java f6/c.java fd/b.java g6/c.java io/familytime/parentalcontrol/models/AppsConfigMainModel.java io/familytime/parentalcontrol/models/LoginEmailModel.java io/familytime/parentalcontrol/models/VpnDataModel.java j1/a.java r5/b.java z6/b.java z6/d.java z8/c.java
5	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	lc/r.java t6/d.java ub/a.java ub/b.java vb/a.java yc/d.java yc/g.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	de/blinkt/openvpn/core/OpenVPNService.java de/blinkt/openvpn/core/OrbotHelper.java de/blinkt/openvpn/core/b.java de/blinkt/openvpn/core/i.java y8/f.java
7	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	q9/b.java sa/c.java
8	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	de/blinkt/openvpn/core/f.java f6/b.java fd/b.java
9	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	a1/v0.java f6/c.java
10	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	io/familytime/parentalcontrol/utils/Utilities.java io/familytime/parentalcontrol/utils/b.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	u4/c.java z4/h.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	x86_64/libopvpnutil.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strncpy_chk']	False warning Symbols are available.
2	x86_64/libbarhopper_v3.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__strlen_chk']	False warning Symbols are available.
3	x86_64/libjbcrypto.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
4	x86_64/libovpnexec.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	x86_64/libovpnutil.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strncpy_chk']	False warning Symbols are available.
6	x86_64/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	False warning Symbols are available.
7	x86_64/libopenvpn.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strrchr_chk', '__strchr_chk', '__strlen_chk', '__vsnprintf_chk', '__memcpy_chk', '__memset_chk', '__strcpy_chk', '__fgets_chk', '__strncpy_chk', '__memmove_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__strcat_chk', '__read_chk', '__umask_chk', '__vsprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86_64/libopvpnutil.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strncpy_chk']	False warning Symbols are available.
9	x86_64/libbarhopper_v3.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__strlen_chk']	False warning Symbols are available.
10	x86_64/libjbcrypto.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
11	x86_64/libovpnexec.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	x86_64/libovpnutil.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strncpy_chk']	False warning Symbols are available.
13	x86_64/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	False warning Symbols are available.
14	x86_64/libopenvpn.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strrchr_chk', '__strchr_chk', '__strlen_chk', '__vsnprintf_chk', '__memcpy_chk', '__memset_chk', '__strcpy_chk', '__fgets_chk', '__strncpy_chk', '__memmove_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__strcat_chk', '__read_chk', '__umask_chk', '__vsprintf_chk']	False warning Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/24	android.permission.INTERNET, android.permission.CAMERA, android.permission.ACCESS_WIFI_STATE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_CONTACTS, android.permission.GET_TASKS
Other Common Permissions	6/45	android.permission.FOREGROUND_SERVICE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.PACKAGE_USAGE_STATS, 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.bouncycastle.org	ok	**IP:** 203.32.61.103 **Country:** Australia **Region:** Victoria **City:** Fitzroy **Latitude:** -37.798389 **Longitude:** 144.978333 **View:** Google Map
android.googlesource.com	ok	**IP:** 142.250.102.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
openvpn.net	ok	**IP:** 104.19.191.106 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
console.firebase.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
www.tiktok.com	ok	**IP:** 2.23.154.130 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
sites.inka.de	ok	**IP:** 193.197.184.17 **Country:** Germany **Region:** Baden-Wurttemberg **City:** Stuttgart **Latitude:** 48.782318 **Longitude:** 9.177020 **View:** Google Map
repo.xposed.info	ok	**IP:** 45.55.233.97 **Country:** United States of America **Region:** New Jersey **City:** Clifton **Latitude:** 40.858429 **Longitude:** -74.163757 **View:** Google Map
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
natmchugh.blogspot.de	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
crowdin.net	ok	**IP:** 52.20.11.191 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
corejr.familytime.io	ok	**IP:** 52.36.170.241 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
maps.google.com	ok	**IP:** 142.251.36.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.tensorflow.org	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
pagead2.googlesyndication.com	ok	**IP:** 142.251.36.226 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
developer.android.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
community.openvpn.net	ok	**IP:** 104.19.191.106 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
xposed.info	ok	**IP:** 45.55.233.97 **Country:** United States of America **Region:** New Jersey **City:** Clifton **Latitude:** 40.858429 **Longitude:** -74.163757 **View:** Google Map
familytime.io	ok	**IP:** 52.41.209.2 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
maximal-cabinet-845.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 195.15.222.169 **Country:** Switzerland **Region:** Basel-Stadt **City:** Basel **Latitude:** 47.558399 **Longitude:** 7.573270 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://maximal-cabinet-845.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
u0013android@android.com u0013android@android.com0	z2/y.java
eay@cryptsoft.com arne@rfc2549.org sales@openvpn.net helbeierling@t-online.de	Android String Resource
android-sdk-releaser@oqei5.prod	lib/x86_64/libbarhopper_v3.so
sales@openvpn.net	lib/x86_64/libopenvpn.so
android-sdk-releaser@oqei5.prod	apktool_out/lib/x86_64/libbarhopper_v3.so
sales@openvpn.net	apktool_out/lib/x86_64/libopenvpn.so

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Pusher		https://reports.exodus-privacy.eu.org/trackers/223

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyAlgz12_IZT3RGH5wRwL-eKvHrBMC-nR7w"
"firebase_database_url" : "https://maximal-cabinet-845.firebaseio.com"
"com.google.firebase.crashlytics.mapping_file_id" : "7c7a798080584a8b931d0c83864cea64"
"auth_username" : "Username"
"password" : "Password"
"settings_auth" : "Authentication/Encryption"
"state_auth" : "Authenticating"
"google_api_key" : "AIzaSyAlgz12_IZT3RGH5wRwL-eKvHrBMC-nR7w"
470fa2b4ae81cd56ecbcda9735803434cec591fa
e2719d58-a985-b3c9-781a-b030af78d30e
9a04f079-9840-4286-ab92-e65be0885f95
7d73d21f1bd82c9e5268b6dcf9fde2cb
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
3071c8717539de5d5353f4c8cd59a032

PLAYSTORE INFORMATION

Title: FamilyTime Jr.

Score: 1.66 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Parenting **Play Store URL:** io.familytime.parentalcontrol

Developer Details: YumyApps, 8018593231756752565, Japan, https://familytime.io/fi/, support@familytime.io,

Release Date: Nov 7, 2017 **Privacy Policy:** Privacy link

Description:

FamilyTime Jr. is a flexible screen time parental control app. It prevents kids from wasting time on smartphones and tablets. With the help of this app, concerned parents can specify when their children can use mobile devices and applications on them. That's why parents need to limit screen time to secure children's health and digital well-being. This parental control app restricts time spent on mobile gadgets and applications. Limit the following device use: • during classes at school • when doing homework • at bedtime or rest hours • when house rules don't allow it Features ★ Internet Schedule - Manage and create a customized schedule to restrict your kid's internet access. ★ Approve Apps - Control which apps can be used on a device by granting or denying permission. ★ Filter the content they can access on the internet and block unwanted site categories with Web Blocker. ★ Use SafeSearch to secure their Google, Bing, and YouTube searches. ★ Set a flexible schedule for the use of apps via the Manage Limits option ★ Individual App Limit - Set specific usage time limits for each app on a device. ★ Parents can monitor their child's social media app activities (WhatsApp, BiP, Instagram, TikTok, YouTube, and more.) ★ Low battery alerts: Receive notifications when the device's battery level is critically low ★ Child can view Blocked Apps or Limited Apps on FamilyTime Jr. App's dashboard ★ TimeBank: Teach your children to bank any unused screen time for later use. ★FunTime - Allow your children to set aside minutes from their daily screen time for fun. ★ Using PickMeUp Alerts, the child can notify the parent/ guardian about the pickup time and location in real time. ★ Review how often your kid uses each app in the Reports section ★ Automatically apply limits to newly added apps. ★ Don't like an app they are using? Block it down. ★ Monitor your kid's location through the Location Tracker, geofencing, and FamilyLocator. ★ Track all SMS messages with the comprehensive SMS tracker. ★ Use the Call Tracker to track calls and view contacts. ★ Your children can generate an SOS alert with one press to send you their GPS location details immediately. ★ The child can unlock the device in the Emergency Unlock feature using the pin provided by the parent. ★ View detailed and actionable reports, including your child's phone usage, location history, and other activity reports. And the best part: it lets you do it all remotely through a parent mobile app or a web control panel created especially for you so you can control your child's safety. Feedback If you have any problems, please look at our help pages or contact us via the contact page of our website since we cannot always help you if you post questions in the reviews. Note: ① This app uses the Device Administrator's permission. ②. To know what information this app collects from the device, check our App Permissions here: https://familytime.io/kb/getting-started/familytime-child-app-permissions-on-android.html. ③. Data charges may apply for using this app over cellular data. Contact your provider for details. ④. Continued use of GPS running in the mobile device's background can drain battery life. ⑤. FamilyTime Jr. requires AccessibilityService API to work Screen Time Limit, App Usage, App Blocker, Daily Limit features, Browser history, Youtube history, or TikTok history. ⑥. FamilyTime Jr. uses VpnService to work Internet Filters, Safe Search, and Safe Internet Features. Those features restrict kids from accessing any inappropriate content. We take your privacy very seriously, and please visit the pages below for more details: ➠ Privacy Policy at https://familytime.io/legal/privacy-policy.html ➠ Terms and Conditions at https://familytime.io/legal/terms-conditions.html

SCAN LOGS

Timestamp	Event	Error
2024-08-15 23:42:58	Generating Hashes	OK
2024-08-15 23:42:58	Extracting APK	OK
2024-08-15 23:42:58	Unzipping	OK
2024-08-15 23:42:58	Getting Hardcoded Certificates/Keystores	OK
2024-08-15 23:43:00	Parsing AndroidManifest.xml	OK

2024-08-15 23:43:00	Parsing APK with androguard	OK
2024-08-15 23:43:01	Extracting Manifest Data	OK
2024-08-15 23:43:01	Performing Static Analysis on: FamilyTime Jr (io.familytime.parentalcontrol)	OK
2024-08-15 23:43:01	Fetching Details from Play Store: io.familytime.parentalcontrol	OK
2024-08-15 23:43:01	Manifest Analysis Started	OK
2024-08-15 23:43:01	Checking for Malware Permissions	OK
2024-08-15 23:43:01	Fetching icon path	OK
2024-08-15 23:43:01	Library Binary Analysis Started	OK
2024-08-15 23:43:01	Analyzing lib/x86_64/libopvpnutil.so	OK
2024-08-15 23:43:01	Analyzing lib/x86_64/libbarhopper_v3.so	OK
2024-08-15 23:43:02	Analyzing lib/x86_64/libjbcrypto.so	OK
2024-08-15 23:43:02	Analyzing lib/x86_64/libovpnexec.so	OK
2024-08-15 23:43:02	Analyzing lib/x86_64/libovpnutil.so	OK
2024-08-15 23:43:02	Analyzing lib/x86_64/libimage_processing_util_jni.so	OK
2024-08-15 23:43:02	Analyzing lib/x86_64/libopenvpn.so	OK

2024-08-15 23:43:04	Analyzing apktool_out/lib/x86_64/libopvpnutil.so	OK
2024-08-15 23:43:04	Analyzing apktool_out/lib/x86_64/libbarhopper_v3.so	OK
2024-08-15 23:43:05	Analyzing apktool_out/lib/x86_64/libjbcrypto.so	OK
2024-08-15 23:43:05	Analyzing apktool_out/lib/x86_64/libovpnexec.so	OK
2024-08-15 23:43:05	Analyzing apktool_out/lib/x86_64/libovpnutil.so	OK
2024-08-15 23:43:05	Analyzing apktool_out/lib/x86_64/libimage_processing_util_jni.so	OK
2024-08-15 23:43:05	Analyzing apktool_out/lib/x86_64/libopenvpn.so	OK
2024-08-15 23:43:07	Reading Code Signing Certificate	OK
2024-08-15 23:43:08	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/cc69bc6bb14ebe2054f3f31fdb64719f/cc69bc6bb14ebe2054f3f31fdb64719f.apk'])
2024-08-15 23:43:08	Running APKiD 2.1.5	OK
2024-08-15 23:43:10	Updating Trackers Database....	OK
2024-08-15 23:43:10	Detecting Trackers	OK
2024-08-15 23:43:12	Decompiling APK to Java with jadx	OK
2024-08-15 23:43:29	Converting DEX to Smali	OK
2024-08-15 23:43:29	Code Analysis Started on - java_source	OK

2024-08-15 23:43:47	Android SAST Completed	OK
2024-08-15 23:43:47	Android API Analysis Started	OK
2024-08-15 23:43:58	Android Permission Mapping Started	OK
2024-08-15 23:44:15	Android Permission Mapping Completed	OK
2024-08-15 23:44:17	Finished Code Analysis, Email and URL Extraction	OK
2024-08-15 23:44:17	Extracting String data from APK	OK
2024-08-15 23:44:17	Extracting String data from SO	OK
2024-08-15 23:44:17	Extracting String data from Code	OK
2024-08-15 23:44:17	Extracting String values and entropies from Code	OK
2024-08-15 23:44:19	Performing Malware check on extracted domains	OK
2024-08-15 23:44:22	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.