MOBSF

ANDROID STATIC ANALYSIS REPORT

FamiSafe Kids (7.2.7.9592)

File Name:	Parental Control App- FamiSafe_merged.apk
Package Name:	com.wondershare.famisafe.kids
Scan Date:	Aug. 11, 2024, 3:54 p.m.

App Security Score: 43/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 8/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
8	30	2	2	3

FILE INFORMATION

File Name: Parental Control App- FamiSafe_merged.apk
Size: 70.34MB

MD5: cf032ae0970af4e8bd46b40c20670364
SHA1: 64a56b04827b7cb9d480325820e847868058f5d3
SHA256: 423d03478f4f0318fbd19a8d75c8e71ef483dc9d3a215b59cd570392f609385f

APP INFORMATION

App Name: FamiSafe Kids
Package Name: com.wondershare.famisafe.kids
Main Activity: com.wondershare.famisafe.kids.activity.SplashKidActivity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 7.2.7.9592
Android Version Code: 9592

APP COMPONENTS

Activities: 56
Services: 22
Receivers: 20
Providers: 4
Exported Activities: 4
Exported Services: 7
Exported Receivers: 10
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-03-30 08:04:51+00:00
Valid To: 2051-03-30 08:04:51+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x1100870bae38eda41b23827ff87b80294cbcedbb
Hash Algorithm: sha256
md5: 604e5e9310ed45263f6d2e06aef9b02d
sha1: 095514ba4f28dbe521c74abf77972be3c86a50a5
sha256: cda673e2e9a696513fdeadaa49cadead966ded389cc2825bdc68afae937928b2
sha512: 892155e9faf4132cb5b3646702609573bc44e29659a2658566f51df487d3fe8021bbe3c44f10a821818d621f2a1ecf72353023987e3c82480e4bf59c4525fa0b
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 6e3a39174d851d88b0ff2dc2e5002634c11d138a73990aa77693ec874c8f59fc
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.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.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.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.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.USE_EXACT_ALARM	normal	allows using exact alarms without user permission.	Allows apps to use exact alarms just like with SCHEDULE_EXACT_ALARM but without needing to request this permission from the user. This is only intended for use by apps that rely on exact alarms for their core functionality. You should continue using SCHEDULE_EXACT_ALARM if your app needs exact alarms for a secondary feature that users may or may not use within your app. Keep in mind that this is a powerful permission and app stores may enforce policies to audit and review the use of this permission. Such audits may involve removal from the app store if the app is found to be misusing this permission.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.wondershare.famisafe.kids.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<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.BRAND check
Build.DEVICE check
Build.PRODUCT check
SIM operator check
network operator name check
ro.kernel.qemu check
possible VM check</td></tr>
<tr><td>Obfuscator</td><td>DexGuard</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>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>

FILE	DETAILS
classes3.dex	FINDINGS: Anti-VM Code — DETAILS: Build.MANUFACTURER check SIM operator check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)
classes4.dex	FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.wondershare.famisafe.kids.activity.SplashKidActivity	Schemes: famisafechrome://, Hosts: com.wondershare.famisafe.kids,
com.wondershare.famisafe.kids.activity.AllowActivity	Schemes: famisafe://, Hosts: com.wondershare.famisafe.kids,
com.sensorsdata.analytics.android.sdk.dialog.SchemeActivity	Schemes: sad3c38eaf://,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.wondershare.famisafe.kids,

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: 2 | WARNING: 21 | 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	Activity (com.wondershare.famisafe.kids.activity.AllowActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (com.sensorsdata.analytics.android.sdk.dialog.SchemeActivity) 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.
5	Service (com.wondershare.famisafe.child.accessibility.SCAccessibilityService) 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	Service (com.wondershare.famisafe.kids.notify.MyNotificationMonitorService) 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.
7	Broadcast Receiver (com.wondershare.famisafe.child.ui.permission.DeviceAdmin) 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.
8	Broadcast Receiver (com.wondershare.famisafe.kids.receiver.myReceiver) 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
9	Broadcast Receiver (com.wondershare.famisafe.kids.receiver.WakeUpReceiver) 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 (com.wondershare.famisafe.kids.receiver.WakeUpReceiver$WakeUpAutoStartReceiver) 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.
11	Broadcast Receiver (com.wondershare.famisafe.kids.livelocation.helper.AlarmReceiver) 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.
12	Broadcast Receiver (com.wondershare.famisafe.kids.accessibility.screenview.ScreenAlarmReceiver) 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 (com.wondershare.famisafe.kids.microrecord.MicroRecordStateAlarmReceiver) 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 (com.wondershare.famisafe.kids.collect.DataSyncAlarmReceiver) 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 (com.appsflyer.SingleInstallBroadcastReceiver) 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	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.
17	Service (com.wondershare.famisafe.kids.MainService) 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.
18	Service (com.wondershare.famisafe.kids.service.WatchDogService) 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.
19	Service (com.wondershare.famisafe.kids.service.WatchDogService$WatchDogNotificationService) 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.
20	Activity (com.wondershare.famsiafe.billing.PayActivity) 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
21	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.
22	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.
23	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.

</> CODE ANALYSIS

HIGH: **5** | WARNING: **8** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a4/g0.java a5/b.java a5/c.java b0/j.java com/adjust/sdk/Logger.java com/airbnb/lottie/LottieAnimationView.java com/alibaba/sdk/android/oss/common/OSSLog.java com/alibaba/sdk/android/oss/common/OSSLogToFileUtils.java com/alibaba/sdk/android/oss/common/auth/OSSFederationToken.java com/alibaba/sdk/android/oss/common/utils/HttpdnsMini.java com/alibaba/sdk/android/oss/network/OSSRequestTask.java com/appsflyer/AFLogger.java com/bumptech/glide/b.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/bitmap_recycle/i.java com/bumptech/glide/load/engine/bitmap_recycle/j.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/c.java com/bumptech/glide/load/resource/bitmap/d.java com/bumptech/glide/load/resource/bitmap/d0.java com/bumptech/glide/load/resource/bitmap/g0.java com/bumptech/glide/load/resource/bitmap/q.java com/bumptech/glide/load/resource/bitmap/r.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/resource/bitmap/v.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/manager/d.java com/bumptech/glide/manager/e.java com/bumptech/glide/request/SingleRequest.java com/contrarywind/view/WheelView.java com/github/mikephil/charting/charts/BarChart.java com/github/mikephil/charting/charts/BarLineChartBase.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/charts/CombinedChart.java com/github/mikephil/charting/charts/HorizontalBarChart.java com/github/mikephil/charting/charts/PieRadarChartBase.java com/github/mikephil/charting/data/PieEntry.java com/github/mikephil/charting/listener/a.java com/littlejie/circleprogress/CircleProgress.java com/magic/player/CustomizablePlayerControlView.java com/magic/player/MediaControllerWrapper.java com/magic/player/PlayerControlView.java com/sensorsdata/analytics/android/autotrack/core/AutoTrackContextHelper.java com/sensorsdata/analytics/android/autotrack/core/autotrack/ActivityLifecycleCallbacks.java com/sensorsdata/analytics/android/autotrack/core/autotrack/FragmentViewScreenCallbacks.java com/sensorsdata/analytics/android/autotrack/core/impl/AutoTrackProtocolIml.java com/sensorsdata/analytics/android/sdk/AbstractSensorsDataAPI.java com/sensorsdata/analytics/android/sdk/AnalyticsMessages.java com/sensorsdata/analytics/android/sdk/SALog.java com/sensorsdata/analytics/android/sdk/SensorsDataAPI.java com/sensorsdata/analytics/android/sdk/advert/deeplink/ChannelDeepLink.java com/sensorsdata/analytics/android/sdk/advert/deeplink/DeepLinkManager.java com/sensorsdata/analytics/android/sdk/advert/impl/SAAdvertProtocolImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/OAIDRom.java com/sensorsdata/analytics/android/sdk/advert/oaid/SAOaidHelper.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/AsusImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/CoolpadImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/HuaweiImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/LenovoImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/MeizuImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/NubiaImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/OAIDFactory.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/OppoImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/SamsungImpl.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/sensorsdata/analytics/android/sdk/advert/oaid/impl/VivoImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/XiaomiImpl.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/ZTEImpl.java com/sensorsdata/analytics/android/sdk/advert/scan/ChannelDebugScanHelper.java com/sensorsdata/analytics/android/sdk/aop/push/PushAutoTrackHelper.java com/sensorsdata/analytics/android/sdk/core/business/SAPluginVersion.java com/sensorsdata/analytics/android/sdk/core/event/imp/BaseEventAssemble.java com/sensorsdata/analytics/android/sdk/core/event/imp/H5TrackAssemble.java com/sensorsdata/analytics/android/sdk/core/event/imp/ItemEventAssemble.java com/sensorsdata/analytics/android/sdk/core/event/imp/StoreDataImpl.java com/sensorsdata/analytics/android/sdk/core/event/imp/TrackEventAssemble.java com/sensorsdata/analytics/android/sdk/core/mediator/SAModuleManager.java com/sensorsdata/analytics/android/sdk/data/SensorsDataDBHelper.java com/sensorsdata/analytics/android/sdk/data/adapter/DataOperation.java com/sensorsdata/analytics/android/sdk/data/adapter/EncryptDataOperation.java com/sensorsdata/analytics/android/sdk/data/adapter/EventDataOperation.java com/sensorsdata/analytics/android/sdk/data/persistent/PersistentSuperProperties.java com/sensorsdata/analytics/android/sdk/dialog/SchemeActivity.java com/sensorsdata/analytics/android/sdk/dialog/SensorsDataDialogUtils.java com/sensorsdata/analytics/android/sdk/encrypt/AESSecretManager.java com/sensorsdata/analytics/android/sdk/encrypt/biz/SecretKeyManager.java com/sensorsdata/analytics/android/sdk/encrypt/encryptor/SAECEncrypt.java com/sensorsdata/analytics/android/sdk/encrypt/impl/SAEncryptAPIImpl.java com/sensorsdata/analytics/android/sdk/encrypt/utils/EncryptUtils.java com/sensorsdata/analytics/android/sdk/exposure/AppPageChange.java com/sensorsdata/analytics/android/sdk/exposure/ExposedPage.java com/sensorsdata/analytics/android/sdk/exposure/ExposedTransform.java com/sensorsdata/analytics/android/sdk/exposure/SAExposedProcess.java com/sensorsdata/analytics/android/sdk/exposure/StayDurationRunnable.java com/sensorsdata/analytics/android/sdk/jsbridge/AppWebViewInterface.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	com/sensorsdata/analytics/android/sdk/jsbridge/JSHookAop.java com/sensorsdata/analytics/android/sdk/network/HttpConfig.java com/sensorsdata/analytics/android/sdk/network/RealRequest.java com/sensorsdata/analytics/android/sdk/plugin/encrypt/AbstractStoreManager.java com/sensorsdata/analytics/android/sdk/plugin/property/PropertyPluginManager.java com/sensorsdata/analytics/android/sdk/push/core/PushProcess.java com/sensorsdata/analytics/android/sdk/remote/BaseSensorsDataSDKRemoteManager.java com/sensorsdata/analytics/android/sdk/remote/SensorsDataRemoteManager.java com/sensorsdata/analytics/android/sdk/remote/SensorsDataRemoteManagerDebug.java com/sensorsdata/analytics/android/sdk/useridentity/Identities.java com/sensorsdata/analytics/android/sdk/useridentity/LoginIDAndKey.java com/sensorsdata/analytics/android/sdk/useridentity/UserIdentityAPI.java com/sensorsdata/analytics/android/sdk/util/AppInfoUtils.java com/sensorsdata/analytics/android/sdk/util/AppStateTools.java com/sensorsdata/analytics/android/sdk/util/DeviceUtils.java com/sensorsdata/analytics/android/sdk/util/NetworkUtils.java com/sensorsdata/analytics/android/sdk/util/Pathfinder.java com/sensorsdata/analytics/android/sdk/util/PermissionUtils.java com/sensorsdata/analytics/android/sdk/util/SADataHelper.java com/sensorsdata/analytics/android/sdk/util/SASchemeHelper.java com/sensorsdata/analytics/android/sdk/util/SASpUtils.java com/sensorsdata/analytics/android/sdk/util/SAViewUtils.java com/sensorsdata/analytics/android/sdk/util/SensorsDataUtils.java com/sensorsdata/analytics/android/sdk/util/ThreadUtils.java com/sensorsdata/analytics/android/sdk/util/ToastUtil.java com/sensorsdata/analytics/android/sdk/util/WebUtils.java com/sensorsdata/analytics/android/sdk/visual/AbstractNodesManager.java com/sensorsdata/analytics/android/sdk/visual/AbstractViewCrawler.java com/sensorsdata/analytics/android/sdk/visual/ViewSnapshot.java com/sensorsdata/analytics/android/sdk/visual/VisualDebugHelper.java com/sensorsdata/analytics/android/sdk/visual/VisualizedAutoTrackService.java com/sensorsdata/analytics/android/sdk/visual/WebViewVisualInterface.java com/sensorsdata/analytics/android/sdk/visual/impl/VisualProtocolImpl.java com/sensorsdata/analytics/android/sdk/visual/property/VisualConfigRequestHelper.java com/sensorsdata/analytics/android/sdk/visual/property/VisualPropertiesCache.java com/sensorsdata/analytics/android/sdk/visual/property/VisualPropertiesManager.java com/sensorsdata/analytics/android/sdk/visual/snap/Caller.java com/sensorsdata/analytics/android/sdk/visual/snap/ResourceReader.java com/sensorsdata/analytics/android/sdk/visual/utils/AlertMessageUtils.java com/sensorsdata/analytics/android/sdk/visual/view/PairingCodeEdit

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Dialog.java com/sensorsdata/analytics/android/sdk/visual/view/PairingCodeRequestHelper.java com/wondershare/famisafe/child/ui/permission/DeviceAdmin.java com/wondershare/famisafe/common/microophone/util/Logger.java com/wondershare/famisafe/common/widget/SimpleRatingBar.java com/wondershare/famisafe/common/widget/WheelView.java com/wondershare/famisafe/common/widget/code/VerificationCodeView.java com/wondershare/famisafe/common/widget/wheel/CustomWheelView.java com/wondershare/famisafe/kids/activity/InterceptionAppActivity.java com/wondershare/famisafe/kids/collect/n.java com/wondershare/famisafe/kids/collect/oss/d.java com/wondershare/famisafe/kids/socialapp/discord/b.java com/wondershare/famisafe/kids/socialapp/discord/d.java com/wondershare/famisafe/kids/socialapp/telegram/TelegramParser.java com/wondershare/famisafe/kids/socialapp/telegram/b.java com/wondershare/famisafe/kids/socialapp/telegram/c.java com/wondershare/famisafe/kids/socialapp/telegram/d.java com/wondershare/famisafe/share/VideoPlayActivity.java com/wondershare/famisafe/share/account/AgreementAct.java com/wondershare/famisafe/share/account/CodeLoginActivity.java f0/a.java f0/c.java f0/h.java f2/a.java f4/j.java h0/c.java h0/d.java h0/j.java h4/m.java i0/d.java j5/b.java j5/f.java k0/i.java k3/a.java k3/e.java k3/g.java k3/h.java l/e.java l3/b.java l4/b.java l4/j.java l5/h.java l6/o1.java l6/t.java m0/b.java m2/a.java n9/j.java o0/a.java org/slf4j/helpers/d.java q/a.java q/b.java r4/d.java r5/b.java r5/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				r9/b.java r9/c.java s5/b.java s5/e.java t/d.java t/e.java t4/f.java t5/k.java v/b.java v/j.java v/l.java v1/p.java v4/b.java v5/g.java w/c.java w/e.java x/e.java x/i.java x1/i.java x5/c.java y/a.java y3/f.java y4/e.java y5/b.java z/c.java z/d.java z/f.java z/s.java z/t.java z5/b.java z5/e.java
2	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	a4/q.java com/alibaba/sdk/android/oss/common/utils/BinaryUtil.java com/appsflyer/internal/ac.java com/sensorsdata/analytics/android/sdk/visual/ViewSnapshot.java com/wondershare/famisafe/kids/collect/oss/OssProxy.java f3/c.java j5/f.java y3/e.java y6/j.java
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/alibaba/sdk/android/oss/common/OSSSQLiteHelper.java com/evernote/android/job/g.java com/sensorsdata/analytics/android/sdk/data/OldBDatabaseHelper.java com/sensorsdata/analytics/android/sdk/data/SensorsDataDBHelper.java o4/b.java p5/a.java t4/b.java t4/e.java t4/f.java t4/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	c9/b.java com/adjust/sdk/Util.java com/appsflyer/internal/e.java d7/e.java d7/h.java f8/e.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/a0.java io/grpc/internal/p1.java io/grpc/okhttp/g.java l4/b.java o7/a.java w8/d.java w8/e.java
5	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/sensorsdata/analytics/android/webview/impl/SAWebViewProtocolImpl.java com/wondershare/famisafe/share/account/AgreementAct.java com/wondershare/famisafe/share/login/WsidWebActivity.java com/wondershare/famsiafe/billing/event/EventDialogFragment.java
6	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/wondershare/famisafe/share/CommonWebActivity.java com/wondershare/famisafe/share/TotalWebActivity.java com/wondershare/famisafe/share/login/WsidWebActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	a3/d.java a4/g0.java a4/r.java a8/b.java b8/c.java c8/a.java com/alibaba/sdk/android/oss/common/utils/HttpdnsMini.java com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java com/wondershare/famisafe/kids/activity/FindParentLocationFragment.java d8/d.java d9/e.java e8/b.java f8/f.java i8/b.java i8/d.java j8/a0.java j8/k.java j8/w.java j8/x.java j8/z.java k8/o.java s7/b.java u7/a.java w7/a.java y6/j.java y7/a.java z7/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/adjust/sdk/Constants.java com/appsflyer/AppsFlyerProperties.java com/appsflyer/CreateOneLinkHttpTask.java com/appsflyer/internal/Exlytics.java com/appsflyer/internal/attribution/RequestErrorMessage.java com/bumptech/glide/load/engine/c.java com/bumptech/glide/load/engine/n.java com/bumptech/glide/load/engine/u.java com/sensorsdata/analytics/android/sdk/advert/utils/ChannelUtils.java com/sensorsdata/analytics/android/sdk/core/mediator/Modules.java com/sensorsdata/analytics/android/sdk/data/adapter/DbParams.java com/sensorsdata/analytics/android/sdk/encrypt/biz/SecretKeyManager.java com/sensorsdata/analytics/android/sdk/encrypt/impl/SAEncryptAPIImpl.java com/sensorsdata/analytics/android/sdk/plugin/encrypt/AbstractStoreManager.java com/sensorsdata/analytics/android/sdk/plugin/encrypt/SAStoreManager.java com/sensorsdata/analytics/android/sdk/useridentity/Identities.java com/sensorsdata/analytics/android/sdk/util/SADataHelper.java com/wondershare/famisafe/common/bean/AppDownloadSwitchBean.java com/wondershare/famisafe/common/bean/ContentManageBean.java com/wondershare/famisafe/common/bean/WebFilterDataBean.java io/grpc/internal/c2.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java l4/d.java u/d.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	u4/a.java
10	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/github/lzyzsd/jsbridge/BridgeWebView.java
11	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/alibaba/sdk/android/oss/common/OSSLogToFileUtils.java com/alibaba/sdk/android/oss/internal/ExtensionRequestOperation.java com/wondershare/famisafe/common/microophone/audio/state/RecordConfig.java com/wondershare/famisafe/kids/collect/n.java f3/a.java k3/d.java k3/g.java l4/b.java x3/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/appsflyer/AppsFlyerLibCore.java com/appsflyer/internal/referrer/GoogleReferrer.java
13	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	com/alibaba/sdk/android/oss/common/utils/BinaryUtil.java com/appsflyer/internal/ac.java com/sensorsdata/analytics/android/sdk/advert/oaid/impl/OppoImpl.java com/wondershare/famisafe/share/payment/g.java f3/c.java v9/b.java
14	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	l5/h.java
15	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/wondershare/famisafe/common/bean/BaseRetrofitManager.java y6/h.java
16	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	y6/a.java
17	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/wondershare/famisafe/share/ABTest.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	mips64/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/libtensorflowlite_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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	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.
3	armeabi-v7a/librsjni_androidx.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
4	armeabi-v7a/libRSSupport.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	armeabi-v7a/libmp3lame.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: ['__vsprintf_chk']	False warning Symbols are available.
6	armeabi-v7a/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
7	armeabi-v7a/librsjni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	x86_64/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
12	x86_64/librsjni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
13	arm64-v8a/libtensorflowlite_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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	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
14	arm64-v8a/librsjni_androidx.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
15	arm64-v8a/libRSSupport.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', '__strlen_chk', '__fgets_chk', '__vsprintf_chk', '__strncat_chk', '__strrchr_chk', '__memcpy_chk']	False warning Symbols are available.
16	arm64-v8a/libmp3lame.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: ['__vsprintf_chk', '__strcat_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	arm64-v8a/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
18	arm64-v8a/librsjni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
19	x86/libtensorflowlite_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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	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
20	x86/librsjni_androidx.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
21	x86/libRSSupport.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
22	x86/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	x86/librsjni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
24	armeabi/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
25	mips/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	mips64/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
27	armeabi-v7a/libtensorflowlite_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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	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.
28	armeabi-v7a/librsjni_androidx.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	armeabi-v7a/libRSSupport.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
30	armeabi-v7a/libmp3lame.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: ['__vsprintf_chk']	False warning Symbols are available.
31	armeabi-v7a/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	armeabi-v7a/librsjni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
33	x86_64/libtensorflowlite_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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	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.
34	x86_64/librsjni_androidx.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
38	arm64-v8a/libtensorflowlite_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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	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.
39	arm64-v8a/librsjni_androidx.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
40	arm64-v8a/libRSSupport.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', '__strlen_chk', '__fgets_chk', '__vsprintf_chk', '__strncat_chk', '__strrchr_chk', '__memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
41	arm64-v8a/libmp3lame.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: ['__vsprintf_chk', '__strcat_chk']	False warning Symbols are available.
42	arm64-v8a/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
43	arm64-v8a/librsjni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
44	x86/libtensorflowlite_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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	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.
45	x86/librsjni_androidx.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
46	x86/libRSSupport.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
47	x86/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
48	x86/librsjni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
49	armeabi/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

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

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	14/24	android.permission.READ_CONTACTS, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.INTERNET, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.SYSTEM_ALERT_WINDOW, android.permission.READ_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.RECORD_AUDIO, android.permission.VIBRATE, android.permission.CAMERA, android.permission.WRITE_EXTERNAL_STORAGE
Other Common Permissions	12/45	android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.CHANGE_WIFI_STATE, android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.ACTIVITY_RECOGNITION, android.permission.ACTIVITY_RECOGNITION, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.PACKAGE_USAGE_STATS, android.permission.BLUETOOTH, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

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
oss-cn-hangzhou.aliyuncs.com	IP: 118.31.219.250 Country: China Region: Zhejiang City: Hangzhou
oss.aliyuncs.com	IP: 118.178.29.5 Country: China Region: Zhejiang City: Hangzhou

DOMAIN MALWARE CHECK

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
sattr.s	ok	No Geolocation information available.
gdpr.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
sadrevenue.s	ok	No Geolocation information available.
gdpr.adjust.com	ok	**IP:** 185.151.204.50 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
lame.sf.net	ok	**IP:** 104.18.20.237 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
analytics.300624.com	ok	**IP:** 47.91.74.43 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
accounts.wondershare.com	ok	**IP:** 47.91.89.51 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
app.adjust.world	ok	**IP:** 185.151.204.42 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
en.wikipedia.org	ok	**IP:** 185.15.59.224 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
data-api.famisafe.com	ok	**IP:** 47.88.22.34 **Country:** United States of America **Region:** California **City:** San Mateo **Latitude:** 37.547424 **Longitude:** -122.330589 **View:** Google Map
subscription.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
famisafe.wondershare.com	ok	**IP:** 104.83.4.144 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
sapp.s	ok	No Geolocation information available.
schemas.android.com	ok	No Geolocation information available.
app.tr.adjust.com	ok	**IP:** 195.244.54.5 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
sgcdsdk.s	ok	No Geolocation information available.
oss-cn-hangzhou.aliyuncs.com	ok	**IP:** 118.31.219.250 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app.adjust.net.in	ok	**IP:** 185.151.204.31 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
subscription.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
app.adjust.com	ok	**IP:** 185.151.204.7 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
subscription.tr.adjust.com	ok	**IP:** 195.244.54.5 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
www.youtube.com	ok	**IP:** 142.251.39.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
image.cnamedomain.com	ok	No Geolocation information available.
sconversions.s	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
famisafe-b6807.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
subscription.adjust.com	ok	**IP:** 185.151.204.52 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
gdpr.tr.adjust.com	ok	**IP:** 195.244.54.5 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
tiktok.com	ok	**IP:** 3.165.206.64 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
subscription.adjust.net.in	ok	**IP:** 185.151.204.34 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
slaunches.s	ok	No Geolocation information available.
svalidate.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
images.phonedata.me	ok	**IP:** 47.246.50.185 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
chrome.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
sonelink.s	ok	No Geolocation information available.
manual.sensorsdata.cn	ok	**IP:** 163.181.50.228 **Country:** Italy **Region:** Lombardia **City:** Milan **Latitude:** 45.464272 **Longitude:** 9.189510 **View:** Google Map
sstats.s	ok	No Geolocation information available.
gdpr.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
youtube.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
ssdk-services.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.250.201.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
famisafeapp.wondershare.com	ok	**IP:** 47.88.22.34 **Country:** United States of America **Region:** California **City:** San Mateo **Latitude:** 37.547424 **Longitude:** -122.330589 **View:** Google Map
gdpr.adjust.world	ok	**IP:** 185.151.204.40 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
subscription.adjust.world	ok	**IP:** 185.151.204.44 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
oss-cn-.aliyuncs.comor	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
oss.aliyuncs.com	ok	**IP:** 118.178.29.5 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dc.wondershare.cc	ok	**IP:** 47.251.13.49 **Country:** United States of America **Region:** California **City:** San Mateo **Latitude:** 37.547424 **Longitude:** -122.330589 **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
api.mapbox.com	ok	**IP:** 18.66.27.107 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
gdpr.adjust.net.in	ok	**IP:** 185.151.204.30 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
app-api-pro.famisafe.com	ok	**IP:** 47.88.22.34 **Country:** United States of America **Region:** California **City:** San Mateo **Latitude:** 37.547424 **Longitude:** -122.330589 **View:** Google Map
127.0.0.1	ok	**IP:** 127.0.0.1 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
sinapps.s	ok	No Geolocation information available.

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://famisafe-b6807.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
system@mail-famisafe.wondershar xiaozw@wondershare.cn	com/wondershare/famisafe/common/data/SpLoacalData.java

TRACKERS

TRACKER	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70

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
Sensors Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/248

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"pref_key_cbp6_default" : "true"
"pref_key_cbp12_title" : "□□"
"pref_key_cbp14_title" : "Alert"
"enter_password" : "Password"
"sus_key_remove_tip" : "□□□□□XXX□□"
"permission_white_doze_key" : "□□□□□□□□□□□□□□□□"
"pref_key_cbp12_title" : "Artículos"
"lbPassword" : "Password"
"pref_key_cbp12_title" : "Resource"
"pref_key_cbp14_title" : "Alerte"
"pref_key_cbp9" : "pref_cbp9"
"pref_key_cbp14_title" : "Avviso"
"pref_key_cbp7" : "pref_cbp7"
"lbPassword" : "□□□□"
"authorization" : "Authorization"
"authorization" : "Autorisierung"

POSSIBLE SECRETS
"enter_password" : "Senha"
"pref_key_cbp13" : "pref_cbp13"
"pref_key_cbp9_default" : "true"
"lbPassword" : "□□□□□□"
"pref_key_cbp13_default" : "true"
"authorization" : "Autorización"
"authorization" : "□□"
"firebase_database_url" : "https://famisafe-b6807.firebaseio.com"
"sus_key_remove_title" : "□□□□□□□□□□"
"reset_password" : "□□□□□□□□□□□□□"
"pref_key_cbp6_default" : "false"
"pref_key_cbp6" : "pref_cbp6"
"enter_your_password" : "□□□□□□□□□□□□□□□□"
"pref_key_cbp14_title" : "Alerta"
"pref_key_cbp14_default" : "true"
"uninstall_user" : "□□□□□□□□□□%s"
"pref_key_cbp14" : "pref_cbp14"
"lbPassword" : "Contraseña"
"authorization" : "Autorizzazione"
"com.google.firebase.crashlytics.mapping_file_id" : "434faeb799ed4581a3e093fe8501798b"
"lbPassword" : "Kennwort"
"pref_key_cbp15_default" : "true"

POSSIBLE SECRETS
"enter_password" : "□□□□□"
"sus_key_remove_setting" : "□□□□□□□□□□"
"pref_key_cbp12_title" : "Articles"
"sus_key_remove_success" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"enter_password" : "□□□□"
"pref_key_cbp14_title" : "□□"
"pref_key_cbp14_title" : "Warnung"
"authorization" : "Autorização"
"google_api_key" : "AIzaSyDXMlASBQ6sbSVZsvZn4N3JHRQpP2WURWU"
"com_facebook_device_auth_instructions" : "facebook.com/device□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"pref_key_cbp12_title" : "Artigos"
"authorization" : "Autorisation"
"pref_key_cbp6_title" : "□□□□□□□□□□□□□□□□□□□□"
"google_crash_reporting_api_key" : "AIzaSyDXMlASBQ6sbSVZsvZn4N3JHRQpP2WURWU"
"com_facebook_device_auth_instructions" : "□□facebook.com/device□□□□□□□□□□□□□□"
"forgetpassword" : "□□□□□□□□□□"
"pref_key_cbp14_title" : "□□□□"
"pref_key_cbp7_title" : "□□□□□□□□□□□□□□"
"enter_password" : "Contraseña"
"pref_key_cbp12_title" : "Articoli"
"pref_key_cbp12_title" : "Beiträge"
"pref_key_cbp7_default" : "true"

POSSIBLE SECRETS
"pref_key_cbp12_default" : "true"
"pref_key_cbp12" : "pref_cbp12"
"account_tip_pwd_length" : "□□□□□□□6□32□□□□□□□□□□□□□□□□□□□□"
"pref_key_cbp9_title" : "□□□□□□□□□□□□□"
"sus_key_remove_setting_tip" : "□□□□□□□□□□□□□□□□□□□□□□□□"
"lbPassword" : "Senha"
"lbforgetpassword" : "□□□□□□□□□□□□□□□"
"pref_key_cbp12_title" : "□□□□□"
"pref_key_cbp15" : "pref_cbp15"
"lbWrongNameOrPassword" : "□□□□□□□□□□□□□□□□□□□□□□□"
"sus_key_remove_setting" : "Erinnerungseinstellungen"
5667676A654B20754F356EA92017D946567C46675556F19556A04616B567D223A5E05656FB549016A96656A557
32879423AB1A0375895786C4BB46E9565FDE0B5344766740AF268ADB32322E5C
ffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551
115792089210356248762697446949407573530086143415290314195533631308867097853951
12511cfe811d0f4e6bc688b4d
47ab8845296aa410f6619e1abad908a1
047B6AA5D85E572983E6FB32A7CDEBC14027B6916A894D3AEE7106FE805FC34B44
3086d221a7d46bcde86c90e49284eb15
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F90F8AA5814A503AD4EB04A8C7DD22CE2826
036b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

POSSIBLE SECRETS
A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7
FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
e4437ed6010e88286f547fa90abfe4c42212
30820268308201d102044a9c4610300d06092a864886f70d0101040500307a310b3009060355040613025553310b30090603550408130243413112301006035504071309506l6c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e3020170d3039303833313231353231365a180f32303530303932353231353231365a307a310b3009060355040613025553310b30090603550408130243413112301006035504071309506l6c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e30819f300d06092a864886f70d010101050003818d0030818902818100c207d51df8eb8c97d93ba0c8c1002c928fab00dc1b42fca5e66e99cc3023ed2d214d822bc59e8e35ddcf5f44c7ae8ade50d7e0c434f500e6c131f4a2834f987fc46406115de2018ebbb0d5a3c261bd97581ccfef76afc7135a6d59e8855ecd7eacc8f8737e794c60a761c536b72b11fac8e603f5da1a2d54aa103b8a13c0dbc10203010001300d06092a864886f70d010104050003818100 5ee9be8bcbb250648d3b741290a82a1c9dc2e76a0af2f2228f1d9f9c4007529c446a70175c5a900d5141812866db46be6559e2141616483998211f4a673149fb2232a10d247663b26a9031e15f84bc1c74d141ff98a02d76f85b2c8ab2571b6469b232d8e768a7f7ca04f7abe4a775615916c07940656b58717457b42bd928a2
64033881142927202683649881450433473985931760268884941288852745803908878638612
0432C4AE2C1F1981195F9904466A39C9948FE30BBFF2660BE1715A4589334C74C7BC3736A2F4F6779C59BDCEE36B692153D0A9877CC62A474002DF32E52139F0A0
000E0D4D696E6768756151750CC03A4473D03679
10E723AB14D696E6768756151756FEBF8FCB49A9
03375D4CE24FDE434489DE8746E71786015009E66E38A926DD
04161FF7528B899B2D0C28607CA52C5B86CF5AC8395BAFEB13C02DA292DDED7A83
00C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E
5363ad4cc05c30e0a5261c028812645a122e22ea20816678df02967c1b23bd72
04017232BA853A7E731AF129F22FF4149563A419C26BF50A4C9D6EEFAD612601DB537DECE819B7F70F555A67C427A8CD9BF18AEB9B56E0C11056FAE6A3
3045AE6FC8422F64ED579528D38120EAE12196D5
6A91174076B1E0E19C39C031FE8685C1CAE040E5C69A28EF
0400FAC9DFCBAC8313BB2139F1BB755FEF65BC391F8B36F8F8EB7371FD558B01006A08A41903350678E58528BEBF8A0BEFF867A7CA36716F7E01F81052
0443BD7E9AFB53D8B85289BCC48EE5BFE6F20137D10A087EB6E7871E2A10A599C710AF8D0D39E2061114FDD05545EC1CC8AB4093247F77275E0743FFED117182EAA9C77877AAAC6AC7D35245D1692E8EE1
151d0f26d4db6decce8842a7dbbe73fb
6C0107475609912222105691 1C77D77E77A777E7E7E77FCB
2AA058F73A0E33AB486B0F610410C53A7F132310

POSSIBLE SECRETS
7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7
1CEF494720115657E18F938D7A7942394FF9425C1458C57861F9EEA6ADBE3BE10
c39c6c3b3a36d7701b9c71a1f5804ae5d0003f4
295F9BAE7428ED9CCC20E7C359A9D41A22FCCD9108E17BF7BA9337A6F8AE9513
D6031998D1B3BBFEBF59CC9BBFF9AEE1
3045AE6FC8422f64ED579528D38120EAE12196D5
0370F6E9D04D289C4E89913CE3530BFDE903977D42B146D539BF1BDE4E9C92
00BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE
00E8BEE4D3E2260744188BE0E9C723
0163F35A5137C2CE3EA6ED8667190B0BC43ECD69977702709B
EE353FCA5428A9300D4ABA754A44C00FDFEC0C9AE4B1A1803075ED967B7BB73F
c49d360886e704936a6678e1139d26b7819f7e90
71169be7330b3038edb025f1
021085E2755381DCCCE3C1557AFA10C2F0C0C2825646C5B34A394CBCFA8BC16B22E7E789E927BE216F02E1FB136A5F
033C258EF3047767E7EDE0F1FDAA79DAEE3841366A132E163ACED4ED2401DF9C6BDCDE98E8E707C07A2239B1B097
D35E472036BC4FB7E13C785ED201E065F98FCFA5B68F12A32D482EC7EE8658E98691555B44C59311
9162fbe73984472a0a9d0590
040369979697AB43897789566789567F787A7876A65400435EDB42EFAFB2989D51FEFCE3C80988F41FF883
74D59FF07F6B413D0EA14B344B20A2DB049B50C3
E87579C11079F43DD824993C2CEE5ED3
29C41E568B77C617EFE5902F11DB96FA9613CD8D03DB08DA
4294182614861580414387344773795550239267234596860714306679811299408947123142002706038521669956384871995765728481489890977075946261343766945636488273037083893479108083593264797677860191534347440096103423131667257868692048219493287863336020338479709268434224762105576023501613261478065276102850944540333865234 1

POSSIBLE SECRETS
340E7BE2A280EB74E2BE61BADA745D97E8F7C300
71FE1AF926CF847989EFEF8DB459F66394D90F32AD3F15E8
bb85691939b869c1d087f601554b96b80cb4f55b35f433c2
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86297
D2C0FB15760860DEF1EEF4D696E6768756151754
00C9517D06D5240D3CFF38C74B20B6CD4D6F9DD4D9
1A827EF00DD6FC0E234CAF046C6A5D8A85395B236CC4AD2CF32A0CADBDC9DDF620B0EB9906D0957F6C6FEACD615468DF104DE296CD8F
0429A0B6A887A983E9730988A68727A8B2D126C44CC2CC7B2A6555193035DC76310804F12E549BDB011C103089E73510ACB275FC312A5DC6B76553F0CA
7CBBBCF9441CFAB76E1890E46884EAE321F70C0BCB4981527897504BEC3E36A62BCDFA2304976540F6450085F2DAE145C22553B465763689180EA2571867423E
216EE8B189D291A0224984C1E92F1D16BF75CCD825A087A239B276D3167743C52C02D6E7232AA
79885141663410976897627118935756323747307951916507639758300472692338873533959
4099B5A457F9D69F79213D094C4BCD4D4262210B
03E5A88919D7CAFCBF415F07C2176573B2
023809B2B7CC1B28CC5A87926AAD83FD28789E81E2C9E3BF10
7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9
004D696E67687561517512D8F03431FCE63B88F4
02A29EF207D0E9B6C55CD260B306C7E007AC491CA1B10C62334A9E8DCD8D20FB7
0108B39E77C4B108BED981ED0E890E117C511CF072
5FF6108462A2DC8210AB403925E638A19C1455D21
7A556B6DAE535B7B51ED2C4D7DAA7A0B5C55F380
00689918DBEC7E5A0DD6DFC0AA55C7

POSSIBLE SECRETS
2E2F85F5DD74CE983A5C4237229DAF8A3F35823BE
04B8266A46C55657AC734CE38F018F2192
072546B5435234A422E0789675F432C89435DE5242
FFFFFFFE0000000075A30D1B9038A115
520883949DFDBC42D3AD198640688A6FE13F41349554B49ACC31DCCD884539816F5EB4AC8FB1F1A6
044BA30AB5E892B4E1649DD0928643ADCD46F5882E3747DEF36E956E97
b8adf1378a6eb73409fa6c9c637ba7f5
B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4
6836319614495570078444416561182725289510217088876144205509505128755031408302 3
044AD5F7048DE709AD51236DE65E4D4B482C836DC6E410664002BB3A02D4AAADACAE24817A4CA3A1B014B5270432DB27D2
030024266E4EB5106D0A964D92C4860E2671DB9B6CC5
043B4C382CE37AA192A4019E763036F4F5DD4D7EBB938CF935318FDCED6BC28286531733C3F03C4FEE
fe0e87005b4e83761908c5131d552a850b3f58b749c37cf5b84d6768
6b016c3bdcf18941d0d654921475ca71a9db2fb27d1d37796185c2942c0a
26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6
7BC86E2102902EC4D5890E8B6B4981ff27E0482750FEFC03
003088250CA6E7C7FE649CE85820F7
1157920892373161954235709850086879078532699846656405640394575840079131296393 19
03188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012
31a92ee2029fd10d901b113e990710f0d21ac6b6
040D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD
00FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681

POSSIBLE SECRETS
e8b4011604095303ca3b8099982be09fcb9ae616
7B425ED097B425ED097B425ED097B425ED097B425ED097B4260B5E9C7710C864
0340340340340340340340340340340340340340340340340340340340323C313FAB50589703B5EC68D3587FEC60D161CC149C1AD4A91
6b8cf07d4ca75c88957d9d67059037a4
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
470fa2b4ae81cd56ecbcda9735803434cec591fa
4D696E676875615175985BD3ADBADA21B43A97E2
0101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA6899164443051D
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA70330870553E5C414CA92619418661197FAC10471DB1D381085DDADDB58796829CA90069
03eea2bae7e1497842f2de7769cfe9c989c072ad696f48034a
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B31F166E6CAC0425A7CF3AB6AF6B7FC3103B883202E9046565
39e9052af60da4c61bb0753b329012ed
1A62BA79D98133A16BBAE7ED9A8E03C32E0824D57AEF72F88986874E5AAE49C27BED49A2A95058068426C2171E99FD3B43C5947C857D
3086d221a7d46bcde86c90e49284eb153dab
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
1335318132727206734338595199483190012179423759678474868994823595993696425287347124615904033277318214103280125292538719147885989931033105677441361963648030647213778266568986864684632777101508094011826087702016153249904683329312949209127762411378780302243557466062839716593764268326742697808800616315281634758887
28091019353058090096996979000309560759124368558014865957655842872397301267595
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
0228F9D04E900069C8DC47A08534FE76D2B900B7D7EF31F5709F200C4CA205
10B7B4D696E676875615175137C8A16FD0DA2211
09f401d7f57ef78f1a2ceee053bb7ff3
0713612DCDDCB40AAB946BDA29CA91F73AF958AFD9

POSSIBLE SECRETS
0402FE13C0537BBC11ACAA07D793DE4E6D5E5C94EEE80289070FB05D38FF58321F2E800536D538CCDAA3D9
00C9BB9E8927D4D64C377E2AB2856A5B16E3EFB7F61D4316AE
6b8cf07d4ca75c88957d9d670591
255705fa2a306654b1f4cb03d6a750a30c250102d4988717d9ba15ab6d3e
A7F561E038EB1ED560B3D147DB782013064C19F27ED27C6780AAF77FB8A547CEB5B4FEF422340353
04015D4860D088DDB3496B0C6064756260441CDE4AF1771D4DB01FFE5B34E59703DC255A868A1180515603AEAB60794E54BB7996A70061B1CFAB6BE5F32BBFA78324ED106A7636B9C5A7BD198D0158AA4F5488D08F38514F1FDF4B4F40D2181B3681C364BA0273C706
036768ae8e18bb92cfcf005c949aa2c6d94853d0e660bbf854b1c9505fe95a
04640ECE5C12788717B9C1BA06CBC2A6FEBA85842458C56DDE9DB1758D39C0313D82BA51735CDB3EA499AA77A7D6943A64F7A3F25FE26F06B51BAA2696FA9035DA5B534BD595F5AF0FA2C892376C84ACE1BB4E3019B71634C01131159CAE03CEE9D9932184BEEF216BD71DF2DADF86A627306ECFF96DBB8BACE198B61E00F8B332
10686D41FF744D4449FCCF6D8EEA03102E6812C93A9D60B978B702CF156D814EF
04BED5AF16EA3F6A4F62938C4631EB5AF7BDBCDBC31667CB477A1A8EC338F94741669C976316DA6321
3FCDA526B6CDF83BA1118DF35B3C31761D3545F32728D003EEB25EFE96
703900853520833051995477180190184378409208826471640810353226014583522983966 01
00E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
0202F9F87B7C574D0BDECF8A22E6524775F98CDEBDCB
C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86294
E8C2505DEDFC86DDC1BD0B2B6667F1DA34B82574761CB0E879BD081CFD0B6265EE3CB090F30D27614CB4574010DA90DD862EF9D4EBEE4761503190785A71C760
07B6882CAAEFA84F9554FF8428BD88E246D2782AE2
9CA8B57A934C54DEEDA9E54A7BBAD95E3B2E91C54D32BE0B9DF96D8D35
3d84f26c12238d7b4f3d516613c1759033b1a5800175d0b1
662C61C430D84EA4FE66A7733D0B76B7BF93EBC4AF2F49256AE58101FEE92B04
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C03

POSSIBLE SECRETS
0409487239995A5EE76B55F9C2F098A89CE5AF8724C0A23E0E0FF77500
0481AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D0098EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9F8227DDE385D566332ECC0EABFA9CF7822FDF209F70024A57B1AA000C55B881F8111B2DCDE494A5F485E5BCA4BD88A2763AED1CA2B2FA8F0540678CD1E0F3AD80892
07A526C63D3E25A256A007699F5447E32AE456B50E
1157920892373161954235709850086879078530737629084992432253781558050790688503 23
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
393C7F7D53666B5054B5E6C6D3DE94F4296C0C599E2E2E241050DF18B6090BDC90186904968BB
3641528A77E9437BDAFABA10DFD532E9
4B337D934104CD7BEF271BF60CED1ED20DA14C08B3BB64F18A60888D
1157920892373161954235709850086879078532699846656405640394575840079131296393 16
02F40E7E2221F295DE297117B7F3D62F5C6A97FFCB8CEFF1CD6BA8CE4A9A18AD84FFABBD8EFA59332BE7AD6756A66E294AFD185A78FF12AA520E4DE739BACA0C7FFEFF7F2955727A
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E24
6A941977BA9F6A435199ACFC51067ED587F519C5ECB541B8E44111DE1D40
1009979067550553047720818155359252248698410825720534578748235158755771479905292727772441528526992987964833566996828420279728960527471731754805904856071347468521419286809125615028022221856475391909026561163678472701450190667942909301854462163997308722217328898303231940973554032134009725883228768509467406639 62
917715298965546059455881490183827502172968583935207241727433257254743749798 01
038D16C2866798B600F9F08BB4A8E860F3298CE04A5798
19020179a6d6f5f7a74e36d7362d2b6e
4D41A619BCC6EADF0448FA22FAD567A9181D37389CA
1420117415975634811963682860223180897432761383952437387628725734419274593935127189736311660784676003608489466235676257952827747192122419290710461342083806363940845126918288940005715246254452957693493567527289568315417754417631393844571917550968471078465956625479423122933384839245143396147277606818806097342 39
04DB4FF10EC057E9AE26B07D0280B7F4341DA5D1B1EAE06C7D9B2F2F6D9C5628A7844163D015BE86344082AA88D95E2F9D
D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F
020A601907B8C953CA1481EB10512F78744A3205FD

POSSIBLE SECRETS
DB7C2ABF62E35E668076BEAD208B
6EE3CEEB230811759F20518A0930F1A4315A827DAC
0405F939258DB7DD90E1934F8C70B0DFEC2EED25B8557EAC9C80E2E198F8CDBECD86B1205303676854FE24141CB98FE6D4B20D02B4516FF702350EDDB0826779C813F0DF45BE8112F4
10C0FB15760860DEF1EEF4D696E676875615175D
5D9306BACD22B7FAEB09D2E049C6E2866C5D1677762A8F2F2DC9A11C7F7BE8340AB2237C7F2A0
114ca50f7a8e2f3f657c1108d9d44cfd8
046AB1E344CE25FF3896424E7FFE14762ECB49F8928AC0C76029B4D5800374E9F5143E568CD23F3F4D7C0D4B1E41C8CC0D1C6ABD5F1A46DB4C
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF
7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CA
041D1C64F068CF45FFA2A63A81B7C13F6B8847A3E77EF14FE3DB7FCAFE0CBD10E8E826E03436D646AAEF87B2E247D4AF1E8ABE1D7520F9C2A45CB1EB8E95CFD55262B70B29FEEC5864E19C054FF99129280E4646217791811142820341263C5315
13D56FFAEC78681E68F9DEB43B35BEC2FB68542E27897B79
64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1
cc22d6dfb95c6b25e49c0d6364a4e5980c393aa21668d953
04B6B3D4C356C139EB31183D4749D423958C27D2DCAF98B70164C97A2DD98F5CFF6142E0F7C8B204911F9271F0F3ECEF8C2701C307E8E4C9E183115A1554062CFB
C49D360886E704936A6678E1139D26B7819F7E90
7d7374168ffe3471b60a857686a19475d3bfa2ff
469A28EF7C28CCA3DC721D044F4496BCCA7EF4146FBF25C9
027B680AC8B8596DA5A4AF8A19A0303FCA97FD7645309FA2A581485AF6263E313B79A2F5
103FAEC74D696E676875615175777FC5B191EF30
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC53
010090512DA9AF72B08349D98A5DD4C7B0532ECA51CE03E2D10F3B7AC579BD87E909AE40A6F131E9CFCE5BD967
1053CDE42C14D696E67687561517533BF3F83345

POSSIBLE SECRETS
127971af8721782ecffa3
51DEF1815DB5ED74FCC34C85D709
D09E8800291CB85396CC6717393284AAA0DA64BA
6277101735386680763835789423207666416083908700390324961279
c56fb7d591ba6704df047fd98f535372fea00211
d8ee438fb4ec6c2b67449ded0ba628cd
0095E9A9EC9B297BD4BF36E059184F
01AF286BCA1AF286BCA1AF286BCA1AF286BCA1AF286BC9FB8F6B85C556892C20A7EB964FE7719E74F490758D3B
0620048D28BCBD03B6249C99182B7C8CD19700C362C46A01
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F0
EE12071A4BC85EE516C78C38E78D1F14
005DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2
1A8F7EDA389B094C2C071E3647A8940F3C123B697578C213BE6DD9E6C8EC7335DCB228FD1EDF4A39152CBCAAF8C0398828041055F94CEEEC7E21340780FE41BD
6127C24C05F38A0AAAF65C0EF02C
0017858FEB7A98975169E171F77B4087DE098AC8A911DF7B01
0021A5C2C8EE9FEB5C4B9A753B7B476B7FD6422EF1F3DD674761FA99D6AC27C8A9A197B272822F6CD57A55AA4F50AE317B13545F
E95E4A5F737059DC60DF5991D45029409E60FC09
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E27
03CE10490F6A708FC26DFE8C3D27C4F94E690134D5BFF988D8D28AAEAEDE975936C66BAC536B18AE2DC312CA493117DAA469C640CAF3
B99B99B099B323E02709A4D696E6768756151751
0400C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14B5E77EFE75928FE1DC127A2FFA8DE3348B3C1856A429BF97E7E31C2E5BD66011839296A789A3BC0045C8A5FB42C7D1BD998F54449579B446817AFBD17273E662C97EE72995EF42640C550B9013FAD0761353C7086A272C24088BE94769FD16650

POSSIBLE SECRETS
57896044618658097711785492504343953926634992332820282019728792003956564823190
85E25BFE5C86226CDB12016F7553F9D0E693A268
e43bb460f0b80cc0c0b075798e948060f8321b7d
E95E4A5F737059DC60DFC7AD95B3D8139515620C
DB7C2ABF62E35E7628DFAC6561C5
0401F481BC5F0FF84A74AD6CDF6FDEF4BF6179625372D8C0C5E10025E399F2903712CCF3EA9E3A1AD17FB0B3201B6AF7CE1B05
401028774D7777C7B7666D1366EA432071274F89FF01E718
002757A1114D696E6768756151755316C05E0BD4
70390085352083305199547718019018437841079516630045180471284346843705633502616
43FC8AD242B0B7A6F3D1627AD5654447556B47BF6AA4A64B0C2AFE42CADAB8F93D92394C79A79755437B56995136
57896044618658097711785492504343953927102133160255826820068844496087732066703
64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1
1E589A8595423412134FAA2DBDEC95C8D8675E58
790408F2EEDAF392B012EDEFB3392F30F4327C0CA3F31FC383C422AA8C16
BDB6F4FE3E8B1D9E0DA8C0D46F4C318CEFE4AFE3B6B8551F
04A3E8EB3CC1CFE7B7732213B23A656149AFA142C47AAFBC2B79A191562E1305F42D996C823439C56D7F7B22E14644417E69BCB6DE39D027001DABE8F35B25C9BE
1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45
040503213F78CA44883F1A3B8162F188E553CD265F23C1567A16876913B0C2AC245849283601CCDA380F1C9E318D90F95D07E5426FE87E45C0E8184698E45962364E34116177DD2259
25FBC363582DCEC065080CA8287AAFF09788A66DC3A9E
0400D9B67D192E0367C803F39E1A7E82CA14A651350AAE617E8F01CE94335607C304AC29E7DEFBD9CA01F596F927224CDECF6C
C2173F1513981673AF4892C23035A27CE25E2013BF95AA33B22C656F277E7335
BD71344799D5C7FCDC45B59FA3B9AB8F6A948BC5

POSSIBLE SECRETS
10D9B4A3D9047D8B154359ABFB1B7F5485B04CEB868237DDC9DEDA982A679A5A919B626D4E50A8DD731B107A9962381FB5D807BF2618
127021248288932417465907042777176443525787653508916535812817507265705031260985098497423188333483401180925999995120988934130659205614996724254121049274349357074920312769561451689224110579311248812610229678534638401693520013288995000362260684222750813532307004517341633685004541062586971416883686778842537820383
2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185EC
2866537B676752636A68F56554E12640276B649EF7526267
044A96B5688EF573284664698968C38BB913CBFC8223A628553168947D59DCC912042351377AC5FB32
703900853520833051995477180190184378410795166300451804712843468437056335026 19
29818893917731240733471273240314769927240550812383695689146495261604565990247
0238af09d98727705120c921bb5e9e26296a3cdcf2f35757a0eafd87b830e7
71169be7330b3038edb025f1d0f9
BB8E5E8FBC115E139FE6A814FE48AAA6F0ADA1AA5DF91985
04B199B13B9B34EFC1397E64BAEB05ACC265FF2378ADD6718B7C7C1961F0991B842443772152C9E0AD
617fab6832576cbbfed50d99f0249c3fee58b94ba0038c7ae84c8c832f2c
043AE9E58C82F63C30282E1FE7BBF43FA72C446AF6F4618129097E2C5667C2223A902AB5CA449D0084B7E5B3DE7CCC01C9
F5CE40D95B5EB899ABBCCFF5911CB8577939804D6527378B8C108C3D2090FF9BE18E2D33E3021ED2EF32D85822423B6304F726AA854BAE07D0396E9A9ADDC40F
040303001D34B856296C16C0D40D3CD7750A93D1D2955FA80AA5F40FC8DB7B2ABDBDE53950F4C0D293CDD711A35B67FB1499AE60038614F1394ABFA3B4C850D927E1E7769C8EEC2D19037BF27342DA639B6DCCFFFEB73D69D78C6C27A6009CBBCA1980F8533921E8A684423E43BAB08A576291AF8F461BB2A8B3531D2F0485C19B16E2F1516E23DD3C1A4827AF1B8AC15B
70B5E1E14031C1F70BBEFE96BDDE66F451754B4CA5F48DA241F331AA396B8D1839A855C1769B1EA14BA53308B5E2723724E090E02DB9
DC9203E514A721875485A529D2C722FB187BC8980EB866644DE41C68E143064546E861C0E2C9EDD92ADE71F46FCF50FF2AD97F951FDA9F2A2EB6546F39689BD3
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC50
10B51CC12849B234C75E6DD2028BF7FF5C1CE0D991A1
0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8
00FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A
02197B07845E9BE2D96ADB0F5F3C7F2CFFBD7A3EB8B6FEC35C7FD67F26DDF6285A644F740A2614

POSSIBLE SECRETS
040081BAF91FDF9833C40F9C181343638399078C6E7EA38C001F73C8134B1B4EF9E150
5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
6BA06FE51464B2BD26DC57F48819BA9954667022C7D03
010092537397ECA4F6145799D62B0A19CE06FE26AD
B4E134D3FB59EB8BAB57274904664D5AF50388BA
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
1854BEBDC31B21B7AEFC80AB0ECD10D5B1B3308E6DBF11C1
00E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D
046B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C2964FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5
07A11B09A76B562144418FF3FF8C2570B8
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FC
9b8f518b086098de3d77736f9458a3d2f6f95a37
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
883423532389192164791648750360308885314476597252960362792450860609699839
B4C4EE28CEBC6C2C8AC12952CF37F16AC7EFB6A9F69F4B57FFDA2E4F0DE5ADE038CBC2FFF719D2C18DE0284B8BFEF3B52B8CC7A5F5BF0A3C8D2319A5312557E1
7503CFE87A836AE3A61B8816E25450E6CE5E1C93ACF1ABC1778064FDCBEFA921DF1626BE4FD036E93D75E6A50E3A41E98028FE5FC235F5B889A589CB5215F2A4
00FDFB49BFE6C3A89FACADAA7A1E5BBC7CC1C2E5D831478814
E2E31EDFC23DE7BDEBE241CE593EF5DE2295B7A9CBAEF021D385F7074CEA043AA27272A7AE602BF2A7B9033DB9ED3610C6FB85487EAE97AAC5BC7928C1950148
7A1F6653786A68192803910A3D30B2A2018B21CD54
04B70E0CBD6BB4BF7F321390B94A03C1D356C21122343280D6115C1D21BD376388B5F723FB4C22DFE6CD4375A05A07476444D5819985007E34
139454871199115825601409655107690713107041707059928031797758001454375765357722984094124368522288239833039114681648076688236921220737322672160740747771700911134550432053804647694904686120113087816240740184800477047157336662926249423571248823968542221753660143391485680840520336859458494803187341288580489525163
5EEEFCA380D02919DC2C6558BB6D8A5D

POSSIBLE SECRETS
96341f1138933bc2f503fd44
36DF0AAFD8B8D7597CA10520D04B
0101BAF95C9723C57B6C21DA2EFF2D5ED588BDD5717E212F9D
5F49EB26781C0EC6B8909156D98ED435E45FD59918
0257927098FA932E7C0A96D3FD5B706EF7E5F5C156E16B7E7C86038552E91D
b3fb3400dec5c4adceb8655d4c94
60dcd2104c4cbc0be6eeefc2bdd610739ec34e317f9b33046c9e4788
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F00
22123dc2395a05caa7423daeccc94760a7d462256bd56916
324A6EDDD512F08C49A99AE0D3F961197A76413E7BE81A400CA681E09639B5FE12E59A109F78BF4A373541B3B9A1
027d29778100c65a1da1783716588dce2b8b4aee8e228f1896
28E9FA9E9D9F5E344D5A9E4BCF6509A7F39789F515AB8F92DDBCBD414D940E93
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F3
985BD3ADBAD4D696E676875615175A21B43A97E3
E95E4A5F737059DC60DFC7AD95B3D8139515620F
04009D73616F35F4AB1407D73562C10F00A52830277958EE84D1315ED31886
4230017757A767FAE42398569B746325D45313AF0766266479B75654E65F
00F50B028E4D696E676875615175290472783FB1
0091A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20
04A1455B334DF099DF30FC28A169A467E9E47075A90F7E650EB6B7A45C7E089FED7FBA344282CAFBD6F7E319F7C0B0BD59E2CA4BDB556D61A5
1AB597A5B4477F59E39539007C7F977D1A567B92B043A49C6B61984C3FE3481AAF454CD41BA1F051626442B3C10

POSSIBLE SECRETS
0403F0EBA16286A2D57EA0991168D4994637E8343E3600D51FBC6C71A0094FA2CDD545B11C5C0C797324F1
287926658148546112969923474583802841350286367782291130057563347309963038881 24
026108BABB2CEEBCF787058A056CBE0CFE622D7723A289E08A07AE13EF0D10D171DD8D
0418DE98B02DB9A306F2AFCD7235F72A819B80AB12EBD653172476FECD462AABFFC4FF191B946A5F54D8D0AA2F418808CC25AB056962D30651A114AFD2755AD336747F93475B7A1FCA3B88F2B6A208CCFE469408584DC2B2912675BF5B 9E582928
06973B15095675534C7CF7E64A21BD54EF5DD3B8A0326AA936ECE454D2C
2472E2D0197C49363F1FE7F5B6DB075D52B6947D135D8CA445805D39BC345626089687742B6329E70680231988
4A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11
0667ACEB38AF4E488C407433FFAE4F1C811638DF20
2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B
04AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB73617DE4A96262C6F5D9E98BF9292DC29F8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C 90EA0E5F
32010857077C5431123A46B808906756F543423E8D27877578125778AC76
0236B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0D
BDB6F4FE3E8B1D9E0DA8C0D40FC962195DFAE76F56564677
3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F723
0066647EDE6C332C7F8C0923BB58213B333B20E9CE4281FE115F7D8F90AD
4E13CA542744D696E67687561517552F279A8C84
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FF
0217C05610884B63B9C6C7291678F9D341
040060F05F658F49C1AD3AB1890F7184210EFD0987E307C84C27ACCFB8F9F67CC2C460189EB5AAAA62EE222EB1B35540CFE902374601E369050B7C4E42ACBA1DACBF04299C3460782F918EA427E6325165E9EA10E3DA5F6C42E9C55215AA9 CA27A5863EC48D8E0286B
04026EB7A859923FBC82189631F8103FE4AC9CA2970012D5D46024804801841CA44370958493B205E647DA304DB4CEB08CBBD1BA39494776FB988B47174DCA88C7E2945283A01C89720349DC807F4FBF374F4AEADE3BCA95314DD58CEC 9F307A54FFC61EFC006D8A2C9D4979C0AC44AEA74FBEBBB9F772AEDCB620B01A7BA7AF1B320430C8591984F601CD4C143EF1C7A3
048BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F046997

POSSIBLE SECRETS
57896044618658097711785492504343953926634992332820282019728792003956564823193
3826F008A8C51D7B95284D9D03FF0E00CE2CD723A
F1FD178C0B3AD58F10126DE8CE42435B53DC67E140D2BF941FFDD459C6D655E1
7fffffffffffffffffffffffff800000cfa7e8594377d414c03821bc582063
0307AF69989546103D79329FCC3D74880F33BBE803CB
3EE30B568FBAB0F883CCEBD46D3F3BB8A2A73513F5EB79DA66190EB085FFA9F492F375A97D860EB4
cc2751449a350f668590264ed76692694a80308a
0289FDFBE4ABE193DF9559ECF07AC0CE78554E2784EB8C1ED1A57A
9ba48cba5ebcb9b6bd33b92830b2a2e0e192f10a
0100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377
659EF8BA043916EEDE8911702B22
03F7061798EB99E238FD6F1BF95B48FEEB4854252B
02120FC05D3C67A99DE161D2F4092622FECA701BE4F50F4758714E8A87BBF2A658EF8C21E7C5EFE965361F6C2999C0C247B0DBD70CE6B7
0452DCB034293A117E1F4FF11B30F7199D3144CE6DFEAFFEF2E331F296E071FA0DF9982CFEA7D43F2E
04925BE9FB01AFC6FB4D3E7D4990010F813408AB106C4F09CB7EE07868CC136FFF3357F624A21BED5263BA3A7A27483EBF6671DBEF7ABB30EBEE084E58A0B077AD42A5A0989D1EE71B1B9BC0455FB0D2C3
04188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF101207192B95FFC8DA78631011ED6B24CDD573F977A11E794811
714114B762F2FF4A7912A6D2AC58B9B5C2FCFE76DAEB7129
7F519EADA7BDA81BD826DBA647910F8C4B9346ED8CCDC64E4B1ABD11756DCE1D2074AA263B88805CED70355A33B471EE
020ffa963cdca8816ccc33b8642bedf905c3d358573d3f27fbbd3b3cb9aaaf
040356DCD8F2F95031AD652D23951BB366A80648F06D867940A5366D9E265DE9EB240F
DB7C2ABF62E35E668076BEAD2088

POSSIBLE SECRETS
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5374
5037EA654196CFF0CD82B2C14A2FCF2E3FF8775285B545722F03EACDB74B
68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43
A335926AA319A27A1D00896A6773A4827ACDAC73
C302F41D932A36CDA7A3462F9E9E916B5BE8F1029AC4ACC1
91E38443A5E82C0D880923425712B2BB658B9196932E02C78B2582FE742DAA28
9a04f079-9840-4286-ab92-e65be0885f95
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C00
77E2B07370EB0F832A6DD5B62DFC88CD06BB84BE
7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ee
0401A57A6A7B26CA5EF52FCDB816479700B3ADC94ED1FE674C06E695BABA1D
c469684435deb378c4b65ca9591e2a5763059a2e
04C0A0647EAAB6A48753B033C56CB0F0900A2F5C4853375FD614B690866ABD5BB88B5F4828C1490002E6773FA2FA299B8F
1243ae1b4d71613bc9f780a03690e
4A6E0856526436F2F88DD07A341E32D04184572BEB710
108576C80499DB2FC16EDDF6853BBB278F6B6FB437D9
24B7B137C8A14D696E6768756151756FD0DA2E5C
687D1B459DC841457E3E06CF6F5E2517B97C7D614AF138BCBF85DC806C4B289F3E965D2DB1416D217F8B276FAD1AB69C50F78BEE1FA3106EFB8CCBC7C5140116

PLAYSTORE INFORMATION

Title: FamiSafe Kids

Score: 1.76 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Parenting **Play Store URL:** com.wondershare.famisafe.kids

Developer Details: Shenzhen Wondershare Software Co., Ltd., Shenzhen+Wondershare+Software+Co.,+Ltd., Room 1204, Building 11A, Shenzhen Bay High-Tech Eco-Park, Keji South Road, Nanshan District, Shenzhen,Guangdong,China, https://famisafe.wondershare.com/, famisafe@wondershare.com,

Release Date: May 19, 2021 **Privacy Policy:** Privacy link

Description:

FamiSafe Kids (formerly FamiSafe Jr - App for kids) is the companion app of the FamiSafe Parental Control App, our app for the parent's device. Please install this FamiSafe Kids onto the devices you want to supervise. Parents need to install FamiSafe Parental Control App on parent devices and then connect this FamiSafe Kids with a pairing code. NEW- SOS Alert: When you are alone outside and feel unsafe, you can quickly seek help from your parents through SOS alert. What you need to do is upgrade FamiSafe to 7.2.0 and turn on this function according to the instructions in the App. FamiSafe Kids allows parents to manage a child's screen time, track a child's location, block inappropriate websites. And other features like game & porn blocking, suspicious photos detecting and suspicious text detecting on social media app like YouTube, Facebook, Instagram, WhatsApp and more. FamiSafe help kids cultivate healthy digital habits and create a safe online environment. Link family devices, keep your family safe. Location Tracker & GPS phone tracker -Track your kids' current location and location history timeline -Create a safe zone for tracking kids and get alerts when they break the planned zone. Phone activity Timeline -Remotely track phone activities -View what apps kids install or uninstall Screen Time Schedule -Track how much screen time kids spend online -Remotely screen time schedule daily or weekly app usage App/Game blocker & Usage -Block or restrict specific inappropriate apps -Send instant alert when children try to open blocked apps or games Website Filter and Brower History -Filter websites to shield kids from porn, gamble or other threatening sites -Track children's browsing history Suspicious Photos Detection -Send instant warnings when detects dangerous pictures in kids' phone albums -View Explicit Images directly on parents' device Suspicious Text Detection -Detect risky keywords from search history, received or sent texts on social media app -Setting keywords you concern about, such as Sex, Violent or Drugs -Detect WhatsApp, Facebook, YouTube, Instagram, Twitter and more How to track screen time, block app/game/porn, filter websites, detect suspicious things with Parental Control App & Location Tracker - FamiSafe? Step 1. Install FamiSafe Parental Control App on parent's device, create an account or log in; Step 2. Install FamiSafe Kids on the device you want to supervise; Step 3. Tie up your kid's device with pairing code and start screen time and parental control! ---FAQs--- • Does FamiSafe Kids phone tracker app work on other platforms? -FamiSafe can protect iPhone, iPad, Kindle devices, and PC (installed on child device) like Windows and Mac OS. • Can parents monitor two or more devices on one account? -Yes. One account can manage up to 30 mobile devices or tablets. If you have any questions, please submit your feedback here: https://famisafe.wondershare.com/ Notes: This app uses the Device Administrator permission. This will prevent a user from uninstalling FamiSafe Kids App without your knowledge. This app uses Accessibility services to build an excellent device experience that helps users with behavioral disabilities set appropriate levels of access and monitoring of screen time, web content and apps, in order to limit their risks and enjoy life normally. Troubleshooting notes: Huawei devices owners: Battery-saving mode needs to be disabled for FamiSafe Kids. ABOUT THE DEVELOPER Wondershare is a global leader in application software development with 15 leading products are used in over 150 countries worldwide and we have over 2 million active users every month. Try for FREE now! After your trial, you can continue to use FamiSafe screen time & parental control app with a monthly subscription.

SCAN LOGS

Timestamp	Event	Error
2024-08-11 15:54:22	Generating Hashes	OK
2024-08-11 15:54:23	Extracting APK	OK
2024-08-11 15:54:23	Unzipping	OK
2024-08-11 15:54:26	Getting Hardcoded Certificates/Keystores	OK
2024-08-11 15:54:58	Parsing AndroidManifest.xml	OK
2024-08-11 15:54:58	Parsing APK with androguard	OK
2024-08-11 15:55:03	Extracting Manifest Data	OK
2024-08-11 15:55:03	Performing Static Analysis on: FamiSafe Kids (com.wondershare.famisafe.kids)	OK

2024-08-11 15:55:03	Fetching Details from Play Store: com.wondershare.famisafe.kids	OK
2024-08-11 15:55:06	Manifest Analysis Started	OK
2024-08-11 15:55:06	Checking for Malware Permissions	OK
2024-08-11 15:55:07	Fetching icon path	OK
2024-08-11 15:55:07	Library Binary Analysis Started	OK
2024-08-11 15:55:07	Analyzing lib/mips64/libpl_droidsonroids_gif.so	OK
2024-08-11 15:55:14	Analyzing lib/armeabi-v7a/libtensorflowlite_jni.so	OK
2024-08-11 15:55:15	Analyzing lib/armeabi-v7a/librsjni_androidx.so	OK
2024-08-11 15:55:16	Analyzing lib/armeabi-v7a/libRSSupport.so	OK
2024-08-11 15:55:27	Analyzing lib/armeabi-v7a/libmp3lame.so	OK
2024-08-11 15:55:29	Analyzing lib/armeabi-v7a/libpl_droidsonroids_gif.so	OK
2024-08-11 15:55:29	Analyzing lib/armeabi-v7a/librsjni.so	OK
2024-08-11 15:55:30	Analyzing lib/x86_64/libtensorflowlite_jni.so	OK
2024-08-11 15:55:31	Analyzing lib/x86_64/librsjni_androidx.so	OK
2024-08-11 15:55:31	Analyzing lib/x86_64/libRSSupport.so	OK

2024-08-11 15:55:40	Analyzing lib/x86_64/libpl_droidsonroids_gif.so	OK
2024-08-11 15:55:41	Analyzing lib/x86_64/librsjni.so	OK
2024-08-11 15:55:41	Analyzing lib/arm64-v8a/libtensorflowlite_jni.so	OK
2024-08-11 15:55:42	Analyzing lib/arm64-v8a/librsjni_androidx.so	OK
2024-08-11 15:55:42	Analyzing lib/arm64-v8a/libRSSupport.so	OK
2024-08-11 15:55:50	Analyzing lib/arm64-v8a/libmp3lame.so	OK
2024-08-11 15:55:52	Analyzing lib/arm64-v8a/libpl_droidsonroids_gif.so	OK
2024-08-11 15:55:52	Analyzing lib/arm64-v8a/librsjni.so	OK
2024-08-11 15:55:53	Analyzing lib/x86/libtensorflowlite_jni.so	OK
2024-08-11 15:55:54	Analyzing lib/x86/librsjni_androidx.so	OK
2024-08-11 15:55:54	Analyzing lib/x86/libRSSupport.so	OK
2024-08-11 15:56:03	Analyzing lib/x86/libpl_droidsonroids_gif.so	OK
2024-08-11 15:56:04	Analyzing lib/x86/librsjni.so	OK
2024-08-11 15:56:04	Analyzing lib/armeabi/libpl_droidsonroids_gif.so	OK
2024-08-11 15:56:04	Analyzing lib/mips/libpl_droidsonroids_gif.so	OK

2024-08-11 15:56:05	Analyzing apktool_out/lib/mips64/libpl_droidsonroids_gif.so	OK
2024-08-11 15:56:12	Analyzing apktool_out/lib/armeabi-v7a/libtensorflowlite_jni.so	OK
2024-08-11 15:56:13	Analyzing apktool_out/lib/armeabi-v7a/librsjni_androidx.so	OK
2024-08-11 15:56:13	Analyzing apktool_out/lib/armeabi-v7a/libRSSupport.so	OK
2024-08-11 15:56:22	Analyzing apktool_out/lib/armeabi-v7a/libmp3lame.so	OK
2024-08-11 15:56:23	Analyzing apktool_out/lib/armeabi-v7a/libpl_droidsonroids_gif.so	OK
2024-08-11 15:56:24	Analyzing apktool_out/lib/armeabi-v7a/librsjni.so	OK
2024-08-11 15:56:24	Analyzing apktool_out/lib/x86_64/libtensorflowlite_jni.so	OK
2024-08-11 15:56:25	Analyzing apktool_out/lib/x86_64/librsjni_androidx.so	OK
2024-08-11 15:56:25	Analyzing apktool_out/lib/x86_64/libRSSupport.so	OK
2024-08-11 15:56:33	Analyzing apktool_out/lib/x86_64/libpl_droidsonroids_gif.so	OK
2024-08-11 15:56:33	Analyzing apktool_out/lib/x86_64/librsjni.so	OK
2024-08-11 15:56:34	Analyzing apktool_out/lib/arm64-v8a/libtensorflowlite_jni.so	OK
2024-08-11 15:56:34	Analyzing apktool_out/lib/arm64-v8a/librsjni_androidx.so	OK
2024-08-11 15:56:34	Analyzing apktool_out/lib/arm64-v8a/libRSSupport.so	OK

2024-08-11 15:56:42	Analyzing apktool_out/lib/arm64-v8a/libmp3lame.so	OK
2024-08-11 15:56:44	Analyzing apktool_out/lib/arm64-v8a/libpl_droidsonroids_gif.so	OK
2024-08-11 15:56:44	Analyzing apktool_out/lib/arm64-v8a/librsjni.so	OK
2024-08-11 15:56:44	Analyzing apktool_out/lib/x86/libtensorflowlite_jni.so	OK
2024-08-11 15:56:45	Analyzing apktool_out/lib/x86/librsjni_androidx.so	OK
2024-08-11 15:56:45	Analyzing apktool_out/lib/x86/libRSSupport.so	OK
2024-08-11 15:56:53	Analyzing apktool_out/lib/x86/libpl_droidsonroids_gif.so	OK
2024-08-11 15:56:53	Analyzing apktool_out/lib/x86/librsjni.so	OK
2024-08-11 15:56:54	Analyzing apktool_out/lib/armeabi/libpl_droidsonroids_gif.so	OK
2024-08-11 15:56:55	Analyzing apktool_out/lib/mips/libpl_droidsonroids_gif.so	OK
2024-08-11 15:56:55	Reading Code Signing Certificate	OK
2024-08-11 15:56:59	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/cf032ae0970af4e8bd46b40c20670364/cf032ae0970af4e8bd46b40c20670364.apk'])
2024-08-11 15:56:59	Running APKiD 2.1.5	OK
2024-08-11 15:57:23	Detecting Trackers	OK

2024-08-11 15:57:42	Decompiling APK to Java with jadx	OK
2024-08-11 15:59:28	Converting DEX to Smali	OK
2024-08-11 15:59:28	Code Analysis Started on - java_source	OK
2024-08-11 16:00:31	Android SAST Completed	OK
2024-08-11 16:00:31	Android API Analysis Started	OK
2024-08-11 16:01:01	Android Permission Mapping Started	OK
2024-08-11 16:08:50	Android Permission Mapping Completed	OK
2024-08-11 16:08:54	Finished Code Analysis, Email and URL Extraction	OK
2024-08-11 16:08:54	Extracting String data from APK	OK
2024-08-11 16:08:55	Extracting String data from SO	OK
2024-08-11 16:08:55	Extracting String data from Code	OK
2024-08-11 16:08:55	Extracting String values and entropies from Code	OK
2024-08-11 16:09:02	Performing Malware check on extracted domains	OK
2024-08-11 16:09:10	Saving to Database	OK