MOBSF

ANDROID STATIC ANALYSIS REPORT

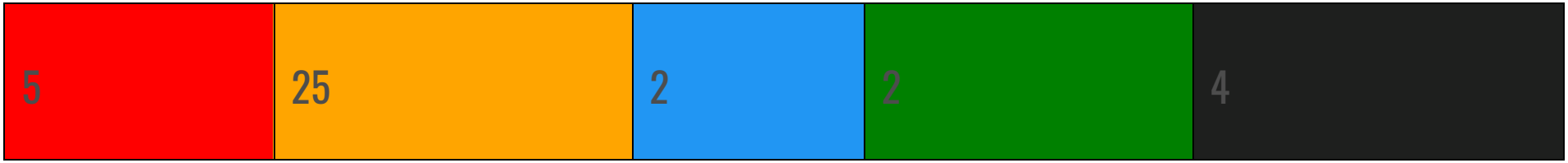
Kidslox (9.6.1)

File Name:	Parental Control - Kidslox_merged.apk
Package Name:	com.kidslox.app

Scan Date:	Aug. 11, 2024, 3:36 p.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	7/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT



FILE INFORMATION

File Name: Parental Control - Kidslox_merged.apk
Size: 29.19MB
MD5: f9bc0a3a21d818f99600c72019c68de8
SHA1: 4bf212ff73bad9bb4d5d88c0ac86c6fe6fd2d478
SHA256: b87b2fb7f747008bb45e6b2cb83974a53afccd4b4c170273a92a38fa783c80fe

APP INFORMATION

App Name: Kidslox
Package Name: com.kidslox.app
Main Activity: com.kidslox.app.activities.SplashActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 9.6.1
Android Version Code: 55139

APP COMPONENTS

Activities: 157
Services: 22
Receivers: 23
Providers: 12
Exported Activities: 5
Exported Services: 3
Exported Receivers: 4
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: C=UK
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-08-20 13:22:15+00:00
Valid To: 2040-08-13 13:22:15+00:00
Issuer: C=UK
Serial Number: 0x4299b1a2
Hash Algorithm: sha256
md5: 995449241abf990b897dd9c03ecb8cb8
sha1: 4bbd8f7e244b86b6b82f2a343ee8edb5e797fef8
sha256: e3814e24acbe3bbfe90ef701d6fdf286adc4cf9ad147be6334e8bb013ce89e62
sha512: 2b33cee6959c5c2be51095cc2cd4ec35f35c03ea58e5e4412bd1bad017007a9faf1cb57257c7064b1184003c468dbbae560d2ac1b7fbb3e72da95276ee96138f
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: fe8ca0d703358902cc7d253a4c7309aeac967375f2447baf386dd43595733abe
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.kidslox.permission.READ_COMMON_PREFERENCES	unknown	Unknown permission	Unknown permission from android reference
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
android.permission.FOREGROUND_SERVICE_SYSTEM_EXEMPTED	normal	allows system-exempted types of foreground services.	Allows a regular application to use Service.startForeground with the type "systemExempted". Apps are allowed to use this type only in the use cases listed in ServiceInfo.FOREGROUND_SERVICE_TYPE_SYSTEM_EXEMPTED .
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	unknown	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
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.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.BROADCAST_CLOSE_SYSTEM_DIALOGS	unknown	Unknown permission	Unknown permission from android reference
BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference
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_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	dangerous	allows reading user-selected image or video files from external storage.	Allows an application to read image or video files from external storage that a user has selected via the permission prompt photo picker. Apps can check this permission to verify that a user has decided to use the photo picker, instead of granting access to READ_MEDIA_IMAGES or READ_MEDIA_VIDEO . It does not prevent apps from accessing the standard photo picker manually. This permission should be requested alongside READ_MEDIA_IMAGES and/or READ_MEDIA_VIDEO , depending on which type of media is desired.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

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.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.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.kidslox.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator check
network operator name check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes4.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
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.kidslox.app.activities.SplashActivity	Schemes: https://, http://, app://, kidslox://, Hosts: kidslox.page.link, com.kidslox.app,
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.com.kidslox.app,
com.stripe.android.link.LinkRedirectHandlerActivity	Schemes: link-popup://, Hosts: complete, Paths: /com.kidslox.app,
com.stripe.android.payments.StripeBrowserProxyReturnActivity	Schemes: stripesdk://, Hosts: payment_return_url, Paths: /com.kidslox.app,

ACTIVITY	INTENT
com.stripe.android.financialconnections.FinancialConnectionsSheetRedirectActivity	Schemes: stripe-auth://, stripe://, Hosts: link-accounts, link-native-accounts, native-redirect, auth-redirect, Paths: /com.kidslox.app/success, /com.kidslox.app/cancel, Path Prefixes: /com.kidslox.app/authentication_return, /com.kidslox.app,
com.google.android.gms.tagmanager.TagManagerPreviewActivity	Schemes: tagmanager.c.com.kidslox.app://,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	mail.kidslox.com	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 15 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	App Link assetlinks.json file not found [android:name=com.kidslox.app.activities.SplashActivity] [android:host=http://kidslox.page.link]	high	App Link asset verification URL (http://kidslox.page.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
4	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.
5	Service (me.pushy.sdk.services.PushyJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
6	Content Provider (com.kidslox.app.providers.CommonPreferencesProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Broadcast Receiver (com.singular.sdk.SingularInstallReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (com.stripe.android.link.LinkRedirectHandlerActivity) 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.
9	Activity (com.stripe.android.payments.StripeBrowserProxyReturnActivity) 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
10	Activity (com.stripe.android.financialconnections.FinancialConnectionsSheetRedirectActivity) 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.
11	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.
12	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.
13	Activity (com.google.android.gms.tagmanager.TagManagerPreviewActivity) 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.
14	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
15	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
16	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
17	High Intent Priority (9991) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: **2** | WARNING: **9** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				coil/memory/MemoryCache.java com/appvestor/android/stats/StatsUtils.java com/appvestor/android/stats/firebase/FirebaseKey.java com/appvestor/android/stats/logging/StatsLogger.java com/kidslox/app/entities/CommandPayload.java com/kidslox/app/entities/Info.java com/kidslox/app/entities/Limitation.java com/kidslox/app/entities/RestrictionsIOS.java com/kidslox/app/entities/User.java com/kidslox/app/entities/VideoHint.java com/kidslox/app/viewmodels/restrictions/RestrictionsStoreViewModel.java com/singular/sdk/internal/BaseApi.java com/singular/sdk/internal/BatchManagerPersistenceSqlite.java com/singular/sdk/internal/Constants.java com/singular/sdk/internal/SingularParamsBase.java com/stripe/android/EphemeralKey.java com/stripe/android/PaymentConfiguration.java com/stripe/android/auth/PaymentBrowserAuthContract.java com/stripe/android/core/networking/ApiRequest.java com/stripe/android/financialconnections/FinancialConnectionsSheet.java com/stripe/android/financialconnections/features/linkaccountpicker/LinkAccountPickerState.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/stripe/android/financialconnections/features/linkstepupverification/LinkStepUpVerificationState.java com/stripe/android/financialconnections/features/networkinglinkverification/NetworkingLinkVerificationState.java com/stripe/android/financialconnections/features/networkingsavetolinkverification/NetworkingSaveToLinkVerificationState.java com/stripe/android/financialconnections/model/FinancialConnectionsSession.java com/stripe/android/financialconnections/model/GetFinancialConnectionsAcccountsParams.java com/stripe/android/googlepaylauncher/GooglePayLauncherContract$PaymentIntentArgs.java com/stripe/android/googlepaylauncher/GooglePayLauncherContract$SetupIntentArgs.java com/stripe/android/model/ConfirmPaymentIntentParams.java com/stripe/android/model/ConfirmSetupIntentParams.java com/stripe/android/model/ConsumerSession.java com/stripe/android/model/ElementsSessionParams.java com/stripe/android/model/FinancialConnectionsSession.java com/stripe/android/model/PaymentIntent.java com/stripe/android/model/PaymentMethodCreateParams.java com/stripe/android/model/SetupIntent.java com/stripe/android/model/Source.java com/stripe/android/model/Stripe3ds2AuthParams.java com/stripe/android/model/Stripe3ds2Fingerprint.java com/stripe/android/model/StripeIntent.java com/stripe/android/model/a.java com/stripe/android/payments/PaymentFlowResult$Unvalidated.java com/stripe/android/payments/bankaccount/navigation/CollectBankAccountContract.java com/stripe/android/payments/bankaccount/ui/a.java com/stripe/android/payments/core/authentication/threeds2/Stripe3ds2TransactionContract.java com/stripe/android/payments/paymentlauncher/PaymentLauncherContract.java com/stripe/android/payments/paymentlauncher/a.java com/stripe/android/paymentsheet/PaymentSheet$CustomerConfiguration.java com/stripe/android/paymentsheet/PaymentSheet$InitializationMode.java com/stripe/android/paymentsheet/addresselement/AddressElementActivityContract$Args.java com/stripe/android/paymentsheet/addresselement/AddressLauncher$Configuration.java com/stripe/android/paymentsheet/d.java com/stripe/android/paymentsheet/paymentdatacollection/ach/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c.java com/stripe/android/paymentsheet/paymentdatacollection/polling/PollingContract.java com/stripe/android/paymentsheet/paymentdatacollection/polling/b.java com/stripe/android/stripe3ds2/transaction/AcsData.java com/stripe/android/stripe3ds2/transaction/AuthenticationRequestParameters.java com/stripe/android/stripe3ds2/transaction/IntentData.java com/stripe/android/uicore/elements/e.java d9/g.java eh/b.java io/purchasely/managers/PLYUserAttributeManager.java io/purchasely/models/PLYImage.java jq/c.java kf/b.java l2/i.java l2/t0.java l7/d.java lf/e.java lf/w.java me/pushy/sdk/config/PushyPreferenceKeys.java me/pushy/sdk/lib/paho/MqttConnectOptions.java me/pushy/sdk/lib/paho/internal/wire/MqttConnack.java me/pushy/sdk/lib/paho/internal/wire/MqttConnect.java me/pushy/sdk/lib/paho/internal/wire/MqttDisconnect.java me/pushy/sdk/lib/paho/internal/wire/MqttPingReq.java me/pushy/sdk/lib/paho/internal/wire/MqttPingResp.java nk/e.java og/g.java or/c.java q0/u0.java v0/e2.java v0/h1.java w8/d.java xv/t0.java z7/n.java zendesk/core/Constants.java zendesk/core/LegacyIdentityMigrator.java zendesk/core/ZendeskCoreSettingsStorage.java zendesk/core/ZendeskIdentityStorage.java zendesk/core/ZendeskMachineIdStorage.java zendesk/core/ZendeskStorage.java zendesk/messaging/MessagingActivity.java zendesk/support/CreateRequest.java zendesk/support/LegacyRequestMigrator.java zendesk/support/ZendeskArticleVoteStorage.java zendesk/support/ZendeskHelpCenterSettingsProvider.java zendesk/support/ZendeskRequestStorage.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				zendesk/support/ZendeskSupportSettingsProvider.java zendesk/support/requestlist/RequestListModel.java zendesk/support/requestlist/RequestListView.java zp/a.java
2	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	me/pushy/sdk/config/PushyStorage.java r9/v0.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	eu/faircode/netguard/ServiceSinkhole.java eu/faircode/netguard/Util.java in/a.java iw/a.java jw/a.java kw/a.java lw/a.java vm/e.java zw/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	a0/b.java a2/m0.java com/appvestor/android/stats/logging/StatsLogger.java com/kidslox/app/entities/NotificationLog.java com/kidslox/app/entities/statistics/ModeChangesLogs.java com/kidslox/app/viewmodels/statistics/b.java com/singular/sdk/Singular.java com/singular/sdk/SingularJSInterface.java com/singular/sdk/internal/BaseApi.java com/singular/sdk/internal/BatchManager.java com/singular/sdk/internal/BatchManagerPersistenceSqlite.java com/singular/sdk/internal/DeviceInfo.java com/singular/sdk/internal/InstallReferrer/SLDigitalTurbineReferrer.java com/singular/sdk/internal/InstallReferrer/SLGoogleReferrer.java com/singular/sdk/internal/LicenseChecker.java com/singular/sdk/internal/ReferrerLinkService.java com/singular/sdk/internal/SingularInstance.java com/singular/sdk/internal/SingularLog.java com/singular/sdk/internal/SingularRequestHandler.java com/singular/sdk/internal/Utils.java de/i.java gf/g.java ib/a.java j9/l.java kb/f0.java lb/c.java lb/k0.java o8/a.java oa/a.java ob/a.java org/tensorflow/lite/NativeInterpreterWrapper.java qk/b.java sb/r.java tc/a.java tx/j.java v2/d.java w2/l.java w2/o.java xd/s.java y2/f.java ya/p.java zendesk/messaging/MessagingModel.java zs/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	ba/w.java h9/j.java l8/c.java n9/b.java
6	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/kidslox/app/activities/WebViewActivity.java io/purchasely/views/PLYWebViewActivity.java
7	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	u4/a.java w/w.java
8	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/singular/sdk/internal/BatchManagerPersistenceSqlite.java com/singular/sdk/internal/SQLitePersistentQueue.java sa/m0.java sa/t0.java x6/c.java
9	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	aa/a.java com/singular/sdk/internal/Utils.java gg/b.java ll/p0.java me/pushy/sdk/lib/paho/internal/websocket/WebSocketHandshake.java
10	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/journeyapps/barcodescanner/d.java com/yellowmessenger/ymchat/YellowBotWebviewFragment.java gg/c.java i6/b.java r7/l0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	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	bv/a.java bv/b.java cv/a.java m/ActivityResultRegistry.java me/pushy/sdk/lib/paho/internal/websocket/WebSocketFrame.java my/c.java p4/p1.java r4/b.java r9/v0.java xg/d.java ya/e.java z4/r.java zb/c.java
12	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	b9/d.java com/airbnb/lottie/network/NetworkCache.java j9/l.java
13	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/yellowmessenger/ymchat/YellowBotWebviewFragment.java
14	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	me/pushy/sdk/lib/paho/internal/security/SSLSocketFactoryFactory.java me/pushy/sdk/util/PushyCertificateManager.java
15	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	de/v.java jf/i.java xd/c.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	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.
2	x86_64/libmlkit_google_ocr_pipeline.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']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	x86_64/libnetguard.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: ['__strcpy_chk', '__vsprintf_chk', '__strlen_chk', '__memcpy_chk']	False warning Symbols are available.
4	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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	x86_64/libmlkit_google_ocr_pipeline.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']	False warning Symbols are available.
6	x86_64/libnetguard.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: ['__strcpy_chk', '__vsprintf_chk', '__strlen_chk', '__memcpy_chk']	False warning Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/24	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.SYSTEM_ALERT_WINDOW, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_PHONE_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA
Other Common Permissions	8/45	android.permission.FOREGROUND_SERVICE, android.permission.PACKAGE_USAGE_STATS, com.google.android.gms.permission.AD_ID, android.permission.READ_CALENDAR, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.ACCESS_BACKGROUND_LOCATION, com.google.android.gms.permission.ACTIVITY_RECOGNITION

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

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
www.baidu.com	IP: 103.235.47.188 Country: Hong Kong Region: Hong Kong City: Hong Kong
www.bing.com	IP: 88.221.92.180 Country: Sri Lanka Region: Western Province City: Colombo

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
m.stripe.com	ok	**IP:** 52.38.209.242 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
www.c	ok	No Geolocation information available.
.facebook.com	ok	No Geolocation information available.
www.language	ok	No Geolocation information available.
traffic.calldorado.com	ok	**IP:** 54.194.140.229 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
accounts.google.com	ok	**IP:** 108.177.96.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
cloud.yellow.ai	ok	**IP:** 104.18.6.105 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
tracking.purchasely.io	ok	**IP:** 104.18.21.12 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
graph-video.s	ok	No Geolocation information available.
stripe.com	ok	**IP:** 198.137.150.141 **Country:** United States of America **Region:** Ohio **City:** Miamisburg **Latitude:** 39.630859 **Longitude:** -84.262108 **View:** Google Map
merchant-ui-api.stripe.com	ok	**IP:** 198.137.150.141 **Country:** United States of America **Region:** Ohio **City:** Miamisburg **Latitude:** 39.630859 **Longitude:** -84.262108 **View:** Google Map
console.firebase.google.com	ok	**IP:** 142.251.39.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.tensorflow.org	ok	**IP:** 142.251.39.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
kidslox.page.link	ok	**IP:** 142.251.39.65 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.stripe.com	ok	**IP:** 34.241.54.72 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
xml.org	ok	**IP:** 104.239.240.11 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
sdk-api-v1.singular.net	ok	**IP:** 95.101.75.49 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.manifestations	ok	No Geolocation information available.
api.purchasely.io	ok	**IP:** 104.18.20.12 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
symbolize.corp.google.com	ok	**IP:** 142.250.27.129 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
kidslox.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
yandex.com	ok	**IP:** 77.88.55.88 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.purchasely.com	ok	**IP:** 199.60.103.29 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.370129 **Longitude:** -71.086304 **View:** Google Map
link.co	ok	**IP:** 18.66.27.28 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.icon	ok	No Geolocation information available.
www.google.com	ok	**IP:** 142.251.208.164 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.baidu.com	ok	**IP:** 103.235.47.188 **Country:** Hong Kong **Region:** Hong Kong **City:** Hong Kong **Latitude:** 22.285521 **Longitude:** 114.157692 **View:** Google Map
duckduckgo.com	ok	**IP:** 40.89.244.232 **Country:** United States of America **Region:** Iowa **City:** Des Moines **Latitude:** 41.600540 **Longitude:** -93.609108 **View:** Google Map
www.googleorganizationautocompleterequirementsconservative	ok	No Geolocation information available.
www.advanced.kidslox.com	ok	**IP:** 52.218.122.148 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
graph.s	ok	No Geolocation information available.
www.world	ok	**IP:** 75.2.38.108 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
errors.stripe.com	ok	**IP:** 198.137.150.91 **Country:** United States of America **Region:** Ohio **City:** Miamisburg **Latitude:** 39.630859 **Longitude:** -84.262108 **View:** Google Map
.jpg	ok	No Geolocation information available.
i.ytimg.com	ok	**IP:** 142.251.208.150 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
twitter.com	ok	**IP:** 104.244.42.129 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
exceptions.singular.net	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.bing.com	ok	**IP:** 88.221.92.180 **Country:** Sri Lanka **Region:** Western Province **City:** Colombo **Latitude:** 6.931940 **Longitude:** 79.847778 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.in	ok	No Geolocation information available.
dashif.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.wencodeuricomponent	ok	No Geolocation information available.
www.hortcut	ok	No Geolocation information available.
checkout.link.com	ok	**IP:** 18.66.27.17 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 142.251.39.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
paywall-staging.purchasely.io	ok	**IP:** 104.18.20.12 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
.css	ok	No Geolocation information available.
goo.gle	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
bi.kidslox.com	ok	**IP:** 34.107.217.205 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api2.amplitude.com	ok	**IP:** 35.155.145.183 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
jsoup.org	ok	**IP:** 188.114.96.11 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
support.link.co	ok	**IP:** 18.66.27.47 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
developers.facebook.com	ok	**IP:** 31.13.84.8 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
www.a	ok	No Geolocation information available.
www.risktabsprev10pxrise25pxblueding300ballfordearnwildbox.fairlackverspairjunetechifpickevil	ok	No Geolocation information available.
www.css	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.tiktok.com	ok	**IP:** 95.101.75.50 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
paywall.purchasely.io	ok	**IP:** 104.18.20.12 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.style	ok	**IP:** 75.2.38.108 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
www.kidslox.com	ok	**IP:** 3.165.206.32 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
tracking-staging.purchasely.io	ok	**IP:** 104.18.20.12 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebase-settings.crashlytics.com	ok	**IP:** 172.217.19.99 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api-staging.purchasely.io	ok	**IP:** 104.18.20.12 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
appleid.apple.com	ok	**IP:** 17.111.105.242 **Country:** United States of America **Region:** California **City:** Cupertino **Latitude:** 37.316605 **Longitude:** -122.046486 **View:** Google Map
facebook.com	ok	**IP:** 31.13.84.36 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
hooks.stripe.com	ok	**IP:** 198.137.150.131 **Country:** United States of America **Region:** Ohio **City:** Miamisburg **Latitude:** 39.630859 **Longitude:** -84.262108 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
admin.kdlparentalcontrol.com	ok	**IP:** 34.120.115.37 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
stats.calldorado.com	ok	**IP:** 52.17.160.169 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.
kidslox.com	ok	**IP:** 3.165.206.126 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.years	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
r5.cloud.yellow.ai	ok	**IP:** 104.18.6.105 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebaseml.googleapis.com	ok	**IP:** 142.251.208.106 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
activity.kdlparentalcontrol.com	ok	**IP:** 142.251.208.115 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
kidsloxsupport.zendesk.com	ok	**IP:** 104.16.51.111 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
firebase.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

DOMAIN	STATUS	GEOLOCATION
ns.adobe.com	ok	No Geolocation information available.
api.pushy.me	ok	**IP:** 35.175.28.61 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.googleapis.com	ok	**IP:** 142.250.180.234 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.250.180.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
search.yahoo.com	ok	**IP:** 212.82.100.137 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
www.interpretation	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
r.stripe.com	ok	**IP:** 54.187.119.242 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
dashboard.stripe.com	ok	**IP:** 198.202.176.141 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.797550 **Longitude:** -73.946190 **View:** Google Map
q.stripe.com	ok	**IP:** 54.187.159.182 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
journeyapps.com	ok	**IP:** 3.165.206.71 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
play.google.com	ok	**IP:** 142.250.180.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app.yellowmessenger.com	ok	**IP:** 104.18.0.51 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
static.afterpay.com	ok	**IP:** 104.16.223.179 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
docs.google.com	ok	**IP:** 142.251.39.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.text-decoration	ok	No Geolocation information available.
bit.ly	ok	**IP:** 67.199.248.10 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
www.recent	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api.eu.amplitude.com	ok	**IP:** 35.157.96.48 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
support.stripe.com	ok	**IP:** 198.202.176.31 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.797550 **Longitude:** -73.946190 **View:** Google Map
tools.android.com	ok	**IP:** 142.251.39.19 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.zendesk.com	ok	**IP:** 104.18.20.26 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS

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

EMAILS

EMAIL	FILE
support@kidslox.com	lk/p0.java
support@kidslox.com	com/kidslox/app/viewmodels/SupportViewModel.java
support@stripe.com	com/stripe/android/core/exception/APIConnectionException.java
support@stripe.com	com/stripe/android/core/networking/ApiRequest.java
support@stripe.com	iq/e.java
help@purchasely.com	io/purchasely/managers/PLYUserManager$startUserTransfer$1.java
support@kidslox.com support@stripe.com	Android String Resource
android-sdk-releaser@ugcia13.prod	lib/x86_64/libmlkit_google_ocr_pipeline.so
android-sdk-releaser@ugcia13.prod	apktool_out/lib/x86_64/libmlkit_google_ocr_pipeline.so

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Analytics, Profiling	https://reports.exodus-privacy.eu.org/trackers/125

TRACKER	CATEGORIES	URL
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
Singular	Analytics	https://reports.exodus-privacy.eu.org/trackers/251

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"zendesk_oauth_client_id" : "mobile_sdk_client_ed45a7620cda87036ee7"
"crashlytics_api_key" : "7662068fa31557f59c2fef70e047d2412c74b161"
"google_crash_reporting_api_key" : "AIzaSyCRXtuzs1zwlhyjeiigWe4uOlUKwMJiWgc"
"firebase_database_url" : "https://kidslox.firebaseio.com"
"mixpanel_token" : "3d740783830e276b027d500a68210e5a"
"singular_secret_key" : "28d2d857304f1e9f8effd8cce66299f2"
"facebook_client_token" : "ac2dfe6ebafb61395124f5bb17e751ae"
"yellow_api_key" : "YxApzgg467n8cmiOg9WZSDQht1zwPLdgU90hOi3g"
"library_zxingandroidembedded_author" : "JourneyApps"

POSSIBLE SECRETS
"monkey" : "Monkey"
"com.google.firebase.crashlytics.mapping_file_id" : "ead7750d4e784d4084b4cada78312244"
"singular_api_key" : "kidslox_0462f4e2"
"stripe_key" : "pk_live_8VdBoYRCy3Ac29HmIWBIB9Zl"
"purchasely_api_key" : "779305c1-01b9-493d-991f-c765c6fa57cf"
"amplitude_api_key" : "7f4a6f5cb79b34ac0f45e1d2d1af6d63"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"uxcam_api_key" : "jozxqkxcozfxu7w"
"google_api_key" : "AIzaSyCRXtuzs1zwlhyjeiigWe4uOlUKwMJiWgc"
"password" : "Password"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166438125740282911150571 51
2758019355995970587784901184038904809305690585636156852142870730198868924130986086513626076488374510776543976123057 5
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
c56fb7d591ba6704df047fd98f535372fea00211
cc2751449a350f668590264ed76692694a80308a
1157920892373161954235709850086879078528375642790749043826051631415181614943 37
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3

POSSIBLE SECRETS
470fa2b4ae81cd56ecbcda9735803434cec591fa
ae2044fb577e65ee8bb576ca48a2f06e
484395612939064517590525852527979142027629495260417479958440807170824046352 86
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
cc4e4752f12ba57046c0d51510d10e3f
115792089210356248762697446949407573530086143415290314195533631308867097853948
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
da67ad7539ab0d638e74781a7909c32c
832571096148902998554675128952010817928785304886131559470920590248050319988441922443864376039294733307808651162787 1
375718002577002046354550722449118360359445513476976248669456777961554447744055631669123440501294553956214444453728942852258566672919658081012434427757837678 4
262470350957996892686231567445669818918529234911092133878156159009255188547380500890223880539757197866508724767320 87
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
115792089237316195423570985008687907853269984665640564039457584007908834671663
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
115792089210356248762697446949407573529996955224135760342422259061068512044369
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
9b8f518b086098de3d77736f9458a3d2f6f95a37

POSSIBLE SECRETS
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
9a04f079-9840-4286-ab92-e65be0885f95
e2719d58-a985-b3c9-781a-b030af78d30e
4105836372515214212932612978004726840911444101599372555483525631403946740129 1
3613425095674979579858512791958788195661110667298501507187719825356841440510 9
5181942b9ebc31ce68dacb56c16fd79f
5506626302227734366957871889516853432625060345377759417550018736038911672924 0
3267051002075881697808308513050704318447127338065924327593890433575733748242 4
52c3345eec7052f0539c991a32e2abb5
dcb428fea25c40e7b99f81ae5981ee6a
deca87e736574c5c83c07314051fd93a
69f94263cfcd124da7d714518f328b40
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186160697311231 9
2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 16
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984

POSSIBLE SECRETS
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3

PLAYSTORE INFORMATION

Title: Parental Control - Kidslox

Score: 4.3265653 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Tools **Play Store URL:** com.kidslox.app

Developer Details: Kidslox, Inc., Kidslox,+Inc., 2035 Sunset Lake Road Suite B-2 Newark Delaware 18702, https://kidslox.com, support@kidslox.com,

Release Date: Aug 21, 2015 **Privacy Policy:** Privacy link

Description:

Kidslox Parental Control App Kidslox parental control and screen time tracker is a secure parental control app that makes it easy for parents to control screen time, track their child's location, block apps, and monitor app usage. Control screen time with Kidslox Parental Control App for all families. Monitor screen time on your child’s device. Address digital wellbeing, monitor app & web activities & lock apps with ease. Kidslox Parental control app features: Our Parental Control app includes a range of tools for monitoring and regulating screen time to help parents manage their kids and teens phone use in line with their desired parenting style: ✔ Instant lock - block your kids apps both on Android & iPhone remotely ✔ Screen time schedules - set fixed times when your child can use their smartphone, e.g. set a bedtime curfew when the phones switch off ✔ Daily time limits - Screen lock & block apps after time limit for a day is reached. ✔ Screen time rewards - give your children extra screen time for completing chores, homework or other tasks ✔ Monitor activities - Parental tracking (parental guidance) has never been so easy - see app usage, check web surfing & sites visited, screen time and more.. ✔ Custom modes - block apps of choice at different times to encourage appropriate behaviour, e.g. allow educational apps during homework but games only during free time Location tracking with Parental monitor ✔ Know your child location via GPS tracking ✔ Get notifications when your child enters or leaves geo-fenced zones you set ✔ See location history and find your kids Easy parental lock & content blocking ✔ Filter pornography and other adult content ✔ Block in-app purchases ✔ Lock safe search on for Google search and other search engines ✔ Full internet blocker Family Parental Controls On All Platforms ✔ Download app for parental control to protect and manage screen time on all your devices ✔ Mobile versions for Android devices and iPhones and iPads ✔ Desktop versions for Windows and Mac ✔ Online, browser based access to controls - turn off junior's phone from your laptop Our parental monitoring app offers several approaches in one simple to use app: For in-the-moment control, use the instant lock. For establishing positive patterns, set daily screen time schedules. When you think your child is ready for a little more freedom, set daily limits. To use Kidslox you will need to download the parenting app onto each device you wish to control. One paid account allows you to control up to 10 devices. Kidslox contains no advertisements. Our support team is ready to help via in-app chat or via email support@kidslox.com. Kidslox offers a 3 day free trial when you sign up. No need to pay until you decide we’re right for you. Learn more about Kidslox on our website: https://kidslox.com Please note: - Kidslox requires an internet connection to operate - This app uses the Device Administrator permission - In order to filter and block undesirable content from your child's device, Kidslox uses a VPN service - To be able to show you what your child is looking at online, take screenshots of their device, and require PIN entry on app deletion, Kidslox requires the Accessibility permission - To be able to show your kids’ positions on a map, Kidslox requires the use of the Location permission on Android phones 8 - Find copies of our terms and conditions here: https://kidslox.com/terms/

SCAN LOGS

Timestamp	Event	Error

2024-08-11 15:36:30	Generating Hashes	OK
2024-08-11 15:36:30	Extracting APK	OK
2024-08-11 15:36:30	Unzipping	OK
2024-08-11 15:36:32	Getting Hardcoded Certificates/Keystores	OK
2024-08-11 15:36:44	Parsing AndroidManifest.xml	OK
2024-08-11 15:36:44	Parsing APK with androguard	OK
2024-08-11 15:36:46	Extracting Manifest Data	OK
2024-08-11 15:36:46	Performing Static Analysis on: Kidslox (com.kidslox.app)	OK
2024-08-11 15:36:46	Fetching Details from Play Store: com.kidslox.app	OK
2024-08-11 15:36:47	Manifest Analysis Started	OK
2024-08-11 15:36:48	Reading Network Security config from network_security_config.xml	OK
2024-08-11 15:36:48	Parsing Network Security config	OK
2024-08-11 15:36:48	Checking for Malware Permissions	OK

2024-08-11 15:36:48	Fetching icon path	OK
2024-08-11 15:36:48	Library Binary Analysis Started	OK
2024-08-11 15:36:48	Analyzing lib/x86_64/libtensorflowlite_jni.so	OK
2024-08-11 15:36:49	Analyzing lib/x86_64/libmlkit_google_ocr_pipeline.so	OK
2024-08-11 15:36:50	Analyzing lib/x86_64/libnetguard.so	OK
2024-08-11 15:36:50	Analyzing apktool_out/lib/x86_64/libtensorflowlite_jni.so	OK
2024-08-11 15:36:51	Analyzing apktool_out/lib/x86_64/libmlkit_google_ocr_pipeline.so	OK
2024-08-11 15:36:52	Analyzing apktool_out/lib/x86_64/libnetguard.so	OK
2024-08-11 15:36:53	Reading Code Signing Certificate	OK
2024-08-11 15:36:54	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/f9bc0a3a21d818f99600c72019c68de8/f9bc0a3a21d818f99600c72019c68de8.apk'])
2024-08-11 15:36:54	Running APKiD 2.1.5	OK
2024-08-11 15:37:23	Detecting Trackers	OK

2024-08-11 15:37:45	Decompiling APK to Java with jadx	OK
2024-08-11 15:41:14	Converting DEX to Smali	OK
2024-08-11 15:41:14	Code Analysis Started on - java_source	OK
2024-08-11 15:44:16	Android SAST Completed	OK
2024-08-11 15:44:16	Android API Analysis Started	OK
2024-08-11 15:46:10	Android Permission Mapping Started	OK
2024-08-11 15:47:26	Android Permission Mapping Completed	OK
2024-08-11 15:47:35	Finished Code Analysis, Email and URL Extraction	OK
2024-08-11 15:47:35	Extracting String data from APK	OK
2024-08-11 15:47:35	Extracting String data from SO	OK
2024-08-11 15:47:35	Extracting String data from Code	OK
2024-08-11 15:47:35	Extracting String values and entropies from Code	OK
2024-08-11 15:47:41	Performing Malware check on extracted domains	OK

2024-08-11 15:47:50	Saving to Database	OK

Report Generated by - MobSF v4.0.6

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.