ANDROID STATIC ANALYSIS REPORT

🤖 **Vitalant (3.4.20240913.1)**

File Name:	org.vitalant.donors_5274.apk
Package Name:	org.vitalant.donors
Scan Date:	Sept. 1, 2025, 5:10 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	5/432

📊 FINDINGS SEVERITY

🐛 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
1	14	5	2	1

📦 FILE INFORMATION

File Name: org.vitalant.donors_5274.apk
Size: 63.47MB
MD5: 76eb9037406085d38382446eedf68c80
SHA1: 7c0d644d15d4ed94771edb3b90f26a36b5fe24a3
SHA256: 40e9abbca3a6cf5f8982f1aaa734e38cd9f0f1f09ddd0f753c980a3f02c986da

ℹ APP INFORMATION

App Name: Vitalant
Package Name: org.vitalant.donors
Main Activity: crc645c7cfcc9932d06f9.MainActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 3.4.20240913.1

Android Version Code: 5274

▞ APP COMPONENTS

Activities: 20
Services: 16
Receivers: 22
Providers: 5
Exported Activities: 0
Exported Services: 3
Exported Receivers: 3
Exported Providers: 0

✺ CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
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: 2021-11-02 18:11:13+00:00
Valid To: 2051-11-02 18:11:13+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x58f8dfa1b6d11112f336598aca2a927a094fbb8
Hash Algorithm: sha256
md5: 064ca5e8742335df10d3d9daad635b1c
sha1: e7b59f7ea7df0b2efa49af7a80c2823bc58e6c27
sha256: 21ca567f9f3118a1138a7ba737a8aa2dce51088bfe64faca5487fcf06b3c40b6
sha512: 03741c7c7f1af38fe7f5a39dc7beff549cfc04abf32f62b780126ff6e43fd41fd23ccd8e96648a444696e76cada0b99e0d87c3a459de38d027d1383581a0ebfa
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 244b83102f31bab46f6a05a539492cf6885e5b9d4cb3084b9d1fb2d4e3a9dc3a
Found 1 unique certificates

⬛ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
org.vitalant.donors.permission.UA_DATA	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.BATTERY_STATS	signature	modify battery statistics	Allows the modification of collected battery statistics. Not for use by common applications.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
org.vitalant.donors.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.

🔍 APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MANUFACTURER check Build.TAGS check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

FILE	DETAILS
classes2.dex	<table><tr><td>FINDINGS</td><td>DETAILS</td></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></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 network operator name check possible VM check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

📑 BROWSABLE ACTIVITIES

ACTIVITY	INTENT
crc645c7cfcc9932d06f9.MainActivity	Schemes: http://, https://, Hosts: vitalantapp.com, vitalant.smart.link, Path Prefixes: /,

🔒 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: **0** | WARNING: **9** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	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.
2	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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	TaskAffinity is set for activity (com.urbanairship.push.NotificationProxyActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
5	Service (io.radar.sdk.RadarJobScheduler) 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	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.

NO	ISSUE	SEVERITY	DESCRIPTION
7	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.
8	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.
9	High Intent Priority (999) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: **0** | WARNING: **4** | INFO: **5** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/kochava/core/log/internal/Logger.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/microsoft/appcenter/AbstractAppCenterService.java
				com/microsoft/appcenter/AppCenter.java
				com/microsoft/appcenter/Constants.java
				com/microsoft/appcenter/Flags.java
				com/microsoft/appcenter/ServiceInstrumentationUtils.java
				com/microsoft/appcenter/UncaughtExceptionHandler.java
				com/microsoft/appcenter/analytics/Analytics.java
				com/microsoft/appcenter/analytics/AnalyticsTransmissionTarget.java
				com/microsoft/appcenter/analytics/AuthenticationProvider.java
				com/microsoft/appcenter/analytics/EventProperties.java
				com/microsoft/appcenter/analytics/channel/AnalyticsValidator.java
				com/microsoft/appcenter/analytics/channel/SessionTracker.java
				com/microsoft/appcenter/analytics/ingestion/models/EventLog.java
				com/microsoft/appcenter/analytics/ingestion/models/json/EventLogFactory.java
				com/microsoft/appcenter/channel/DefaultChannel.java
				com/microsoft/appcenter/channel/OneCollectorChannelListener.java
				com/microsoft/appcenter/crashes/Crashes.java
				com/microsoft/appcenter/crashes/WrapperSdkExceptionManager.java
				com/microsoft/appcenter/crashes/ingestion/models/AbstractErrorLog.java
				com/microsoft/appcenter/crashes/ingestion/models/ErrorAttachmentLog.java
				com/microsoft/appcenter/crashes/ingestion/models/HandledErrorLog.java
				com/microsoft/appcenter/crashes/ingestion/models/ManagedErrorLog.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java
				com/microsoft/appcenter/http/AbstractAppCallTemplate.java
				com/microsoft/appcenter/http/DefaultHttpClient.java
				com/microsoft/appcenter/http/DefaultHttpClientCallTask.java
				com/microsoft/appcenter/http/HttpClientNetworkStateHandler.java
				com/microsoft/appcenter/http/HttpClientRetryer.java
				com/microsoft/appcenter/ingestion/OneCollectorIngestion.java
				com/microsoft/appcenter/ingestion/models/AbstractLog.java
				com/microsoft/appcenter/ingestion/models/one/CommonSchemaDataUtils.java
				com/microsoft/appcenter/ingestion/models/one/CommonSchemaLog.java
				com/microsoft/appcenter/ingestion/models/one/PartAUtils.java
				com/microsoft/appcenter/persistence/DatabasePersistence.java
				com/microsoft/appcenter/utils/AppCenterLog.java
				com/microsoft/appcenter/utils/AsyncTaskUtils.java
				com/microsoft/appcenter/utils/DeviceInfoHelper.java
				com/microsoft/appcenter/utils/IdHelper.java
				com/microsoft/appcenter/utils/NetworkStateHelper.java
				com/microsoft/appcenter/utils/context/SessionContext.java
				com/microsoft/appcenter/utils/context/UserIdContext.java
				com/microsoft/appcenter/utils/crypto/CryptoUtils.java
				com/microsoft/appcenter/utils/storage/DatabaseManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/microsoft/appcenter/utils/storage/File Manager.java
				com/urbanairship/AirshipConfigOptions.java
				com/urbanairship/Autopilot.java
				com/urbanairship/ChannelCapture.java
				com/urbanairship/DefaultLogHandler.java
				com/urbanairship/DeferredPlatformProvider.java
				com/urbanairship/Fonts.java
				com/urbanairship/PreferenceDataStore.java
				com/urbanairship/PushProviders.java
				com/urbanairship/UALog.java
				com/urbanairship/UAirship.java
				com/urbanairship/UrlAllowList.java
				com/urbanairship/actions/Action.java
				com/urbanairship/actions/ActionEntryParser.java
				com/urbanairship/actions/ActionRunRequest.java
				com/urbanairship/actions/AddCustomEventAction.java
				com/urbanairship/actions/DeepLinkAction.java
				com/urbanairship/actions/OpenExternalUrlAction.java
				com/urbanairship/actions/PermissionResultReceiver.java
				com/urbanairship/actions/PromptPermissionAction.java
				com/urbanairship/actions/RateAppActivity.java
				com/urbanairship/actions/SetAttributesAction.java
				com/urbanairship/actions/SubscriptionListAction.java
				com/urbanairship/actions/WalletAction.java
				com/urbanairship/actions/WalletLoadingActivity.java
				com/urbanairship/actions/tags/AddTagsAction.java
				com/urbanairship/actions/tags/RemoveTags

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Action.java com/urbanairship/analytics/Analytics.java com/urbanairship/analytics/AssociateIdentifiersEvent.java com/urbanairship/analytics/CustomEvent.java com/urbanairship/analytics/Event.java com/urbanairship/analytics/InstallReceiver.java com/urbanairship/analytics/ScreenTrackingEvent.java com/urbanairship/analytics/data/AnalyticsDatabase.java com/urbanairship/analytics/data/EventApiClient.java com/urbanairship/analytics/data/EventDao.java com/urbanairship/analytics/data/EventManager.java com/urbanairship/analytics/location/CircularRegion.java com/urbanairship/analytics/location/ProximityRegion.java com/urbanairship/analytics/location/RegionEvent.java com/urbanairship/android/layout/environment/AttributeHandler.java com/urbanairship/android/layout/gestures/PagerGestureMapper.java com/urbanairship/android/layout/model/BaseFormController$initParentForm$2.java com/urbanairship/android/layout/model/BaseModel.java com/urbanairship/android/layout/model/PagerModel.java com/urbanairship/android/layout/property/HexColor.java com/urbanairship/android/layout/reporting/DisplayTimer.java com/urbanairship/android/layout/ui/LayoutBanner.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/urbanairship/android/layout/ui/LayoutViewModel.java
				com/urbanairship/android/layout/ui/ModalActivity.java
				com/urbanairship/android/layout/view/MediaView.java
				com/urbanairship/android/layout/view/WebViewView.java
				com/urbanairship/audience/AudienceHash.java
				com/urbanairship/audience/AudienceHashSelector.java
				com/urbanairship/audience/AudienceSelector.java
				com/urbanairship/audience/BucketSubset.java
				com/urbanairship/automation/AutomationEngine.java
				com/urbanairship/automation/InAppAutomation.java
				com/urbanairship/automation/InAppRemoteDataObserver.java
				com/urbanairship/automation/NetworkMonitor.java
				com/urbanairship/automation/RemoteDataAccess.java
				com/urbanairship/automation/alarms/AlarmOperationScheduler.java
				com/urbanairship/automation/limits/FrequencyLimitManager.java
				com/urbanairship/automation/storage/AutomationDaoWrapper.java
				com/urbanairship/automation/storage/Converters.java
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/urbanairship/automation/storage/LegacyDataManager.java
				com/urbanairship/automation/storage/LegacyDataMigrator.java
				com/urbanairship/channel/AirshipChannel.java
				com/urbanairship/channel/AttributeEditor.ja

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/urbanairship/channel/AttributeEditor.java
				com/urbanairship/channel/AttributeMutation.java
				com/urbanairship/channel/ChannelApiClient.java
				com/urbanairship/channel/ChannelBatchUpdateApiClient.java
				com/urbanairship/channel/ChannelRegistrar.java
				com/urbanairship/channel/ChannelRegistrationPayload.java
				com/urbanairship/channel/SubscriptionListApiClient.java
				com/urbanairship/channel/SubscriptionListEditor.java
				com/urbanairship/channel/SubscriptionListMutation.java
				com/urbanairship/channel/TagGroupsEditor.java
				com/urbanairship/channel/TagUtils.java
				com/urbanairship/contacts/Contact.java
				com/urbanairship/contacts/ContactApiClient.java
				com/urbanairship/contacts/ContactManager.java
				com/urbanairship/contacts/ScopedSubscriptionListEditor.java
				com/urbanairship/contacts/ScopedSubscriptionListMutation.java
				com/urbanairship/contacts/SubscriptionListApiClient.java
				com/urbanairship/db/RecoverableMigration.java
				com/urbanairship/experiment/EvaluationOptions.java
				com/urbanairship/experiment/Experiment.java
				com/urbanairship/experiment/ExperimentManager.java
				com/urbanairship/experiment/ExperimentResult.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				esult.java com/urbanairship/experiment/MessageCriteria.java com/urbanairship/google/PlayServicesErrorActivity.java com/urbanairship/google/PlayServicesUtils.java com/urbanairship/http/Response.java com/urbanairship/iam/AdapterWrapper.java com/urbanairship/iam/DisplayHandler.java com/urbanairship/iam/InAppActivityMonitor.java com/urbanairship/iam/InAppMessage.java com/urbanairship/iam/InAppMessageActivity.java com/urbanairship/iam/InAppMessageManager.java com/urbanairship/iam/LegacyInAppMessageManager.java com/urbanairship/iam/TextInfo.java com/urbanairship/iam/actions/LandingPageAction.java com/urbanairship/iam/assets/AirshipPrepareAssetsDelegate.java com/urbanairship/iam/assets/AssetCache.java com/urbanairship/iam/assets/AssetManager.java com/urbanairship/iam/assets/Assets.java com/urbanairship/iam/banner/BannerAdapter.java com/urbanairship/iam/html/HtmlActivity.java com/urbanairship/iam/html/HtmlDisplayAdapter.java com/urbanairship/iam/html/HtmlWebViewClient.java com/urbanairship/iam/layout/AirshipLayoutDisplayAdapter.java com/urbanairship/iam/view/InAppViewUtils.java com/urbanairship/images/ImageCache.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/urbanairship/images/ImageCache.java
				com/urbanairship/images/ImageRequest.java
				com/urbanairship/javascript/JavaScriptEnvironment.java
				com/urbanairship/javascript/NativeBridge.java
				com/urbanairship/job/AirshipWorker.java
				com/urbanairship/job/JobDispatcher.java
				com/urbanairship/job/JobRunner.java
				com/urbanairship/json/JsonExtensionsKt.java
				com/urbanairship/json/JsonList.java
				com/urbanairship/json/JsonMap.java
				com/urbanairship/json/JsonTypeConverters.java
				com/urbanairship/json/JsonValue.java
				com/urbanairship/locale/LocaleChangeReceiver.java
				com/urbanairship/locale/LocaleManager.java
				com/urbanairship/messagecenter/Inbox.java
				com/urbanairship/messagecenter/InboxApiClient.java
				com/urbanairship/messagecenter/InboxJobHandler.java
				com/urbanairship/messagecenter/MessageActivity.java
				com/urbanairship/messagecenter/MessageCenter.java
				com/urbanairship/messagecenter/MessageCenterActivity.java
				com/urbanairship/messagecenter/MessageDao.java
				com/urbanairship/messagecenter/MessageEntity.java
				com/urbanairship/messagecenter/MessageFragment.java
				com/urbanairship/messagecenter/User.java
				com/urbanairship/modules/Modules.java
				com/urbanairship/permission/PermissionsA

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ctivity.java com/urbanairship/permission/Permissions Manager.java
				com/urbanairship/permission/SinglePermiss ionDelegate.java com/urbanairship/push/ActionButtonGroup sParser.java com/urbanairship/push/IncomingPushRunn able.java com/urbanairship/push/NotificationIntentPr ocessor.java com/urbanairship/push/NotificationProxyAc tivity.java com/urbanairship/push/NotificationProxyRe ceiver.java com/urbanairship/push/PushManager.java com/urbanairship/push/PushMessage.java com/urbanairship/push/PushProviderBridge .java com/urbanairship/push/fcm/FcmPushProvid er.java com/urbanairship/push/notifications/Notific ationActionButtonGroup.java com/urbanairship/push/notifications/Notific ationChannelCompat.java com/urbanairship/push/notifications/Notific ationChannelRegistry.java com/urbanairship/push/notifications/Notific ationChannelRegistryDataManager.java com/urbanairship/push/notifications/Notific ationChannelUtils.java com/urbanairship/push/notifications/Notific ationUtils.java com/urbanairship/push/notifications/Public NotificationExtender.java com/urbanairship/push/notifications/StyleN otificationExtender.java com/urbanairship/push/notifications/Weara bleNotificationExtender.java com/urbanairship/remoteconfig/ModuleAda pter.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/urbanairship/remoteconfig/RemoteConfigManager$updateSubscription$1.java com/urbanairship/remoteconfig/RemoteConfigManager.java com/urbanairship/remotedata/RemoteData.java com/urbanairship/remotedata/RemoteDataProvider.java com/urbanairship/remotedata/RemoteDataStore.java com/urbanairship/util/ConnectionUtils.java com/urbanairship/util/DataManager.java com/urbanairship/util/FileUtils.java com/urbanairship/util/HelperActivity.java com/urbanairship/util/ImageUtils.java com/urbanairship/util/Network.java com/urbanairship/util/NotificationIdGenerator.java com/urbanairship/util/ProcessUtils.java com/urbanairship/util/PropertiesConfigParser.java com/urbanairship/util/UAStringUtil.java com/urbanairship/wallet/Pass.java com/urbanairship/wallet/PassRequest.java com/urbanairship/webkit/AirshipWebChromeClient.java com/urbanairship/webkit/AirshipWebView.java com/urbanairship/webkit/AirshipWebViewClient.java io/radar/sdk/RadarActivityLifecycleCallbacks.java io/radar/sdk/RadarLogger.java mono/android/incrementaldeployment/IncrementalClassLoader.java
				com/microsoft/appcenter/AppCenter.java com/microsoft/appcenter/Constants.java com/microsoft/appcenter/channel/DefaultChannel.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java com/microsoft/appcenter/http/DefaultHttpClient.java com/microsoft/appcenter/ingestion/OneCollectorIngestion.java com/microsoft/appcenter/ingestion/models/WrapperSdk.java com/microsoft/appcenter/ingestion/models/one/CommonSchemaLog.java com/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/utils/context/SessionContext.java com/microsoft/appcenter/utils/storage/DatabaseManager.java com/urbanairship/AirshipConfigOptions.java com/urbanairship/ApplicationMetrics.java com/urbanairship/Autopilot.java com/urbanairship/DeferredPlatformProvider.java com/urbanairship/PreferenceDataDatabase.java com/urbanairship/PrivacyManager.java com/urbanairship/UAirship.java com/urbanairship/actions/ClipboardAction.java com/urbanairship/actions/FetchDeviceInfoAction.java com/urbanairship/actions/PromptPermissionAction.java com/urbanairship/actions/RateAppAction.java com/urbanairship/actions/SetAttributesAction.java com/urbanairship/actions/SubscriptionListAction.java com/urbanairship/actions/ToastAction.java com/urbanairship/actions/tags/BaseTagsAction.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/urbanairship/analytics/Analytics.java com/urbanairship/analytics/AppForeground Event.java
				com/urbanairship/analytics/AssociatedIdenti fiers.java
				com/urbanairship/analytics/Event.java
				com/urbanairship/analytics/InteractiveNotifi cationEvent.java
				com/urbanairship/analytics/PushArrivedEve nt.java
				com/urbanairship/analytics/ScreenTrackingE vent.java
				com/urbanairship/analytics/data/EventMana ger.java
				com/urbanairship/analytics/location/Locatio nEvent.java
				com/urbanairship/android/layout/property/ StateAction.java
				com/urbanairship/audience/AudienceSelecto r.java
				com/urbanairship/automation/InAppAutoma tion.java
				com/urbanairship/automation/InAppRemote DataObserver.java
				com/urbanairship/automation/ScheduleDela y.java
				com/urbanairship/automation/Trigger.java com/urbanairship/automation/TriggerConte xt.java
				com/urbanairship/automation/actions/Sche duleAction.java
				com/urbanairship/automation/deferred/Def erred.java
				com/urbanairship/automation/deferred/Def erredScheduleClient.java
				com/urbanairship/automation/deferred/Stat eOverrides.java
				com/urbanairship/automation/storage/Lega cyDataMigrator.java
				com/urbanairship/channel/AirshipChannel.ja

NO	ISSUE	SEVERITY	STANDARDS	FILES
				va com/urbanairship/channel/AttributeMutation.java
2	[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/urbanairship/channel/ChannelApiClient.java com/urbanairship/channel/ChannelBatchUpdateManager.java com/urbanairship/channel/ChannelRegistrar.java com/urbanairship/channel/ChannelRegistrationPayload.java com/urbanairship/channel/TagGroupsMutation.java com/urbanairship/config/RemoteAirshipUrlConfigProvider.java com/urbanairship/contacts/AssociatedChannel.java com/urbanairship/contacts/Contact.java com/urbanairship/contacts/ContactApiClient.java com/urbanairship/contacts/ContactData.java com/urbanairship/contacts/ContactIdentity.java com/urbanairship/contacts/ContactManager.java com/urbanairship/contacts/ContactOperation.java com/urbanairship/contacts/EmailRegistrationOptions.java com/urbanairship/contacts/OpenChannelRegistrationOptions.java com/urbanairship/contacts/SmsRegistrationOptions.java com/urbanairship/contacts/SubscriptionListApiClient.java com/urbanairship/http/RequestAuth.java com/urbanairship/iam/ButtonInfo.java com/urbanairship/iam/DisplayContent.java com/urbanairship/iam/InAppMessage.java com/urbanairship/iam/InAppMessageActivit

NO	ISSUE	SEVERITY	STANDARDS	FILES
				y.java com/urbanairship/iam/InAppMessageManager.java com/urbanairship/iam/LegacyInAppMessage.java com/urbanairship/iam/MediaInfo.java com/urbanairship/iam/ResolutionInfo.java com/urbanairship/iam/TextInfo.java com/urbanairship/iam/actions/LandingPageAction.java com/urbanairship/iam/assets/AirshipPrepareAssetsDelegate.java com/urbanairship/iam/banner/BannerDisplayContent.java com/urbanairship/iam/custom/CustomDisplayContent.java com/urbanairship/iam/events/InAppReportingEvent.java com/urbanairship/iam/html/HtmlDisplayContent.java com/urbanairship/iam/layout/AirshipLayoutDisplayContent.java com/urbanairship/javascript/NativeBridge.java com/urbanairship/json/JsonMatcher.java com/urbanairship/json/matchers/ArrayContainsMatcher.java com/urbanairship/json/matchers/ExactValueMatcher.java com/urbanairship/json/matchers/NumberRangeMatcher.java com/urbanairship/json/matchers/PresenceMatcher.java com/urbanairship/json/matchers/VersionMatcher.java com/urbanairship/locale/LocaleManager.java com/urbanairship/location/AirshipLocationManager.java com/urbanairship/location/LocationRequest

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Options.java com/urbanairship/messagecenter/InboxApiClient.java
				com/urbanairship/messagecenter/Message.java
				com/urbanairship/messagecenter/MessageDatabase.java
				com/urbanairship/messagecenter/User.java
				com/urbanairship/push/NotificationsPermissionDelegate.java
				com/urbanairship/push/PushManager.java
				com/urbanairship/push/PushMessage.java
				com/urbanairship/push/QuietTimeInterval.java
				com/urbanairship/push/notifications/NotificationChannelCompat.java
				com/urbanairship/push/notifications/PublicNotificationExtender.java
				com/urbanairship/push/notifications/StyleNotificationExtender.java
				com/urbanairship/push/notifications/WearableNotificationExtender.java
				com/urbanairship/remoteconfig/DisableInfo.java
				com/urbanairship/remoteconfig/RemoteAirshipConfig.java
				com/urbanairship/remoteconfig/RemoteConfigManager.java
				com/urbanairship/remotedata/RemoteData.java
				com/urbanairship/remotedata/RemoteDataProvider.java
				com/urbanairship/util/Attributes.java
				com/urbanairship/util/NotificationIdGenerator.java
				com/urbanairship/util/VersionUtils.java
				com/urbanairship/wallet/Field.java
				com/urbanairship/wallet/Pass.java
3	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/urbanairship/wallet/PassRequest.javaDat aProviderHelper/RandState.javaper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/utils/storage/DatabaseManager.java com/urbanairship/automation/storage/LegacyDataManager.java com/urbanairship/push/notifications/NotificationChannelRegistryDataManager.java com/urbanairship/remotedata/RemoteDataStore.java com/urbanairship/util/DataManager.java
5	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/urbanairship/ChannelCapture.java com/urbanairship/actions/ClipboardAction.java
6	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	com/microsoft/appcenter/http/HttpClientRetryer.java com/urbanairship/remotedata/RemoteData.java
7	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	io/radar/sdk/RadarSettings.java io/radar/sdk/RadarState.java io/radar/sdk/RadarUtils.java
8	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/urbanairship/util/ImageUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	[This app listens to Clipboard changes. Some malware also listen to Clipboard changes.](#)	info	OWASP MASVS: MSTG-PLATFORM-4	crc64a0e0a82d0db9a07d/ClipboardChangeListener.java mono/android/content/ClipboardManager_OnPrimaryClipChangedListenerImplementor.java
10	This App uses SQL Cipher. Ensure that secrets are not hardcoded in code.	info	OWASP MASVS: MSTG-CRYPTO-1	com/microsoft/appcenter/utils/storage/DatabaseManager.java

🔒 NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

📊 BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/urbanairship/UAirship.java com/urbanairship/actions/DeepLinkAction.java com/urbanairship/actions/OpenExternalUrlAction.java com/urbanairship/actions/PromptPermissionAction.java com/urbanairship/actions/WalletAction.java com/urbanairship/actions/WalletLoadingActivity.java com/urbanairship/push/PushMessage.java com/urbanairship/util/AppStoreUtils.java com/urbanairship/wallet/Pass.java com/urbanairship/webkit/AirshipWebChromeClient.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/urbanairship/actions/PromptPermissionAction.java com/urbanairship/actions/WalletAction.java com/urbanairship/wallet/Pass.java
00016	Get location info of the device and put it to JSON object	location collection	io/radar/sdk/Radar.java io/radar/sdk/RadarApiClient.java io/radar/sdk/model/RadarEvent.java io/radar/sdk/model/RadarUser.java
00022	Open a file from given absolute path of the file	file	com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/microsoft/appcenter/crashes/Crashes.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java com/microsoft/appcenter/utils/storage/FileManager.java com/urbanairship/PreferenceDataDatabase.java com/urbanairship/analytics/data/AnalyticsDatabase.java com/urbanairship/automation/limits/storage/FrequencyLimitDatabase.java com/urbanairship/automation/storage/AutomationDatabase.java com/urbanairship/iam/assets/AirshipPrepareAssetsDelegate.java com/urbanairship/iam/assets/Assets.java com/urbanairship/messagecenter/MessageDatabase.java com/urbanairship/util/DataManager.java com/urbanairship/util/FileUtils.java com/urbanairship/util/ImageUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00005	Get absolute path of file and put it to JSON object	file	com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java
00004	Get filename and put it to JSON object	file collection	com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java
00036	Get resource file from res/raw directory	reflection	com/urbanairship/AirshipConfigOptions.java com/urbanairship/UAirship.java com/urbanairship/actions/PromptPermissionAction.java com/urbanairship/push/PushMessage.java com/urbanairship/push/notifications/NotificationChannelCompat.java com/urbanairship/util/AppStoreUtils.java
00091	Retrieve data from broadcast	collection	com/kochava/tracker/engagement/Engagement.java com/urbanairship/push/notifications/NotificationActionButton.java io/radar/sdk/RadarForegroundService.java
00013	Read file and put it into a stream	file	com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/microsoft/appcenter/utils/storage/FileManager.java okio/Okio.java
00078	Get the network operator name	collection telephony	com/microsoft/appcenter/utils/DeviceInfoHelper.java com/urbanairship/util/Network.java
00132	Query The ISO country code	telephony collection	com/microsoft/appcenter/utils/DeviceInfoHelper.java
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/kochava/core/network/base/internal/NetworkBaseRequest.java
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/kochava/core/network/base/internal/NetworkBaseRequest.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/kochava/tracker/store/meta/internal/MetaUtil.java
00072	Write HTTP input stream into a file	command network file	com/urbanairship/util/FileUtils.java
00108	Read the input stream from given URL	network command	com/urbanairship/util/FileUtils.java
00089	Connect to a URL and receive input stream from the server	command network	com/kochava/core/network/base/internal/NetworkBaseRequest.java
00109	Connect to a URL and get the response code	network command	com/kochava/core/network/base/internal/NetworkBaseRequest.java

🗄 FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/282153882064/namespaces/firebase:fetch?key=AIzaSyCFyag3zU74WF179Pz7nJan_OgTNjkzL9Q. This is indicated by the response: {'state': 'NO_TEMPLATE'}

⣿ ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.CAMERA, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_WIFI_STATE
Other Common Permissions	6/44	android.permission.BATTERY_STATS, android.permission.ACCESS_BACKGROUND_LOCATION, com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.c2dm.permission.RECEIVE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

❗ OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
int.dewrain.world	ok	**IP:** 34.160.223.119 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** [Google Map](#)
combine.urbanairship.com	ok	**IP:** 34.107.195.75 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** [Google Map](#)
device-api.asnapieu.com	ok	**IP:** 130.211.7.30 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** [Google Map](#)
int.akisinn.info	ok	**IP:** 34.160.223.119 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
mobile.events.data.microsoft.com	ok	**IP:** 13.70.79.200 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map
combine.asnapieu.com	ok	**IP:** 35.244.242.208 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
int.dewrain.life	ok	**IP:** 34.160.223.119 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
int.kvaedit.site	ok	**IP:** 35.244.187.134 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
wallet-api.urbanairship.com	ok	**IP:** 35.244.226.117 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
device-api.urbanairship.com	ok	**IP:** 34.128.138.27 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
.asnapieu.com	ok	No Geolocation information available.
docs.airship.com	ok	**IP:** 34.107.238.88 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
smart.link	ok	**IP:** 34.36.249.118 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
api-verified.radar.io	ok	**IP:** 104.16.50.56 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
.urbanairship.com	ok	No Geolocation information available.
www.youtube.com	ok	**IP:** 172.217.21.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
token.api.kochava.com	ok	**IP:** 34.36.239.136 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
radar.com	ok	**IP:** 34.217.231.110 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
remote-data.asnapieu.com	ok	**IP:** 34.96.96.216 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
int.dewrain.site	ok	**IP:** 34.160.223.119 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
kvinit-prod.api.kochava.com	ok	**IP:** 34.160.223.119 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
int.akisinn.site	ok	**IP:** 34.160.223.119 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
remote-data.urbanairship.com	ok	**IP:** 34.144.204.212 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
int.vaicore.site	ok	**IP:** 34.160.223.119 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
int.vaicore.store	ok	**IP:** 34.160.223.119 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
int.vaicore.xyz	ok	**IP:** 34.160.223.119 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
in.appcenter.ms	ok	**IP:** 4.152.45.207 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
wallet-api.asnapieu.com	ok	**IP:** 34.96.86.174 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
control.kochava.com	ok	**IP:** 107.178.254.148 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.radar.io	ok	**IP:** 104.17.35.116 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

🕵 TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Microsoft Visual Studio App Center Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/243
Microsoft Visual Studio App Center Crashes	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/238
Radar		https://reports.exodus-privacy.eu.org/trackers/288
Urbanairship		https://reports.exodus-privacy.eu.org/trackers/123

🔑 HARDCODED SECRETS

POSSIBLE SECRETS

"google_api_key" : "AIzaSyCFyag3zU74WF179Pz7nJan_OgTNjkzL9Q"

"google_crash_reporting_api_key" : "AIzaSyCFyag3zU74WF179Pz7nJan_OgTNjkzL9Q"

c69d1dc2f3bcc22522abf71ffd5f8c91

c103703e120ae8cc73c9248622f3cd1e

35dc8997e1e42159a519f7f02410cda8

1146f4c5ff2c986072906aee3af2535f

3082024d308201b6a00302010202044f31d2cb300d06092a864886f70d0101050500306a310b30090603550406130255533113301106035504081308130a43616c69666f726e6961311630140603550407130d53616e204672616e636973636f31116301406035504081308130a496e7374616672616d20496e6331163014060355040313d4b6576696e6e2053797374726f6d3020170d3132303230383031343133315a180f3231313323031313530314341313315a306a310b30090603550406130255533113301106035504081308130a43616c69666f726e6961311630140603550407130d53616e204672616e636973636f31116301406035504081308130a496e7374616672616d20496e6331163014060355040313d4b6576696e6e2053797374726f6d30819f300d06092a864886f70d010101050003818d003081890281810089ebcac015660b42a5c080bf694c52e29e9df83a4c94964b022ca38d2ba2157d8e4650955c787906ac344bdb8b7d202a92231403d48e9e2f0df3cb917cfa9b9741314c85052673d42ad00f2c251be4a6b012fb9d5b33131b0e5ca0b9193856dc311dc65dc45f97d2632e72bec2b4964adfd5d30675d5d372fbaf11359a7afb550203010001300d06092a864886f70d0101050500038181002aefd84526b570192967b679a685bcdc12cf40030589594d04d885cfa8a311372fb93f2c1c8ba636f061aeb87207f5a1ad26fe58747c30714f1e9b918ab2e090d5250307655eeab5fede1e6409316c5d29779c037b550f29bcad40fa70c947b616cc05daa5532c0ecc3ece773a71f37287a4ac32f2bd7feede847cbac5671969

AndroidHorizontalListViewRenderer+DragAnDropItemTouchHelperCallback

79c080bb2cc94348ebcb15fce911dd4b

867ae7d13f0985895f1665a5fc7b7a17

4bfc112e4986489ec8dd7db647ee82f8

207c96f5c0531578ea783ce59c607d01

POSSIBLE SECRETS

30820268308201d102044a9c4610300d06092a864886f70d0101040500307a310b30090603550406130255533310b3009060355040813024341311230100060355040713 0950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b06035504031314466163 65626f6f6b20436f72706f726174696f6e3020170d30393038333313231353231365a180f32303530303932353231353231365a307a310b30090603550406130255533310b 300906035504081302434131123010060355040713095610616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b13084 6616365626f6f6b311d301b06035504031314466616365626f6f6b20436f72706f726174696f6e30819f300d06092a864886f70d010101050003818d0030818902818100c2 07d51df8eb8c97d93ba0c8c1002c928fab00dc1b42fca5e66e99cc3023ed2d214d822bc59e8e35ddcf5f44c7ae8ade50d7e0c434f500e6c131f4a2834f987fc46406115de20 18ebbb0d5a3c261bd97581ccfef76afc7135a6d59e8855ecd7eacc8f8737e794c60a761c536b72b11fac8e603f5da1a2d54aa103b8a13c0dbc10203010001300d06092a864 886f70d0101040500038181005ee9be8bcbb250648d3b741290a82a1c9dc2e76a0af2f2228f1d9f9c4007529c446a70175c5a900d5141812866db46be6559e2141616483 998211f4a673149fb2232a10d247663b26a9031e15f84bc1c74d141ff98a02d76f85b2c8ab2571b6469b232d8e768a7f7ca04f7abe4a775615916c07940656b58717457b4 2bd928a2

93e1ac461cee9254319cdc372fa539bf

---

d9f9d711f596d7f406febbe363d73f40

400933b7a06a2d0cdaabbefb93b3eecc

49f946663a8deb7054212b8adda248c6

▶ PLAYSTORE INFORMATION

Title: Vitalant

Score: 4.2929688 **Installs:** 50,000+ **Price:** 0 **Android Version Support: Category:** Medical **Play Store URL:** org.vitalant.donors

Developer Details: Vitalant, Vitalant, None, https://www.vitalant.org, supportapp@vitalant.org,

Release Date: Mar 31, 2022 **Privacy Policy:** Privacy link

Description:

The Vitalant Blood Donor App makes saving lives easy and convenient. Schedule and manage appointments, access your donation history, find nearby donation centers, and track your health info—all in one place. Get push notification reminders and stay updated on urgent donation needs. Download now to make a difference!

☰ SCAN LOGS

Timestamp	Event	Error
2025-09-01 17:10:58	Generating Hashes	OK
2025-09-01 17:10:58	Extracting APK	OK
2025-09-01 17:10:58	Unzipping	OK
2025-09-01 17:10:58	Parsing APK with androguard	OK
2025-09-01 17:10:58	Extracting APK features using aapt/aapt2	OK
2025-09-01 17:10:58	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 17:11:00	Parsing AndroidManifest.xml	OK
2025-09-01 17:11:00	Extracting Manifest Data	OK
2025-09-01 17:11:00	Manifest Analysis Started	OK

2025-09-01 17:11:00	Performing Static Analysis on: Vitalant (org.vitalant.donors)	OK
2025-09-01 17:11:02	Fetching Details from Play Store: org.vitalant.donors	OK
2025-09-01 17:11:03	Checking for Malware Permissions	OK
2025-09-01 17:11:03	Fetching icon path	OK
2025-09-01 17:11:03	Library Binary Analysis Started	OK
2025-09-01 17:11:03	Reading Code Signing Certificate	OK
2025-09-01 17:11:04	Running APKiD 2.1.5	OK
2025-09-01 17:11:07	Detecting Trackers	OK
2025-09-01 17:11:09	Decompiling APK to Java with JADX	OK
2025-09-01 17:11:25	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 17:11:25	Decompiling classes2.dex with JADX	OK

2025-09-01 17:11:35	Decompiling classes.dex with JADX	OK
2025-09-01 17:11:44	Decompiling with JADX failed for classes.dex	OK
2025-09-01 17:11:44	Decompiling classes2.dex with JADX	OK
2025-09-01 17:11:54	Decompiling classes.dex with JADX	OK
2025-09-01 17:12:02	Some DEX files failed to decompile	OK
2025-09-01 17:12:02	Converting DEX to Smali	OK
2025-09-01 17:12:02	Code Analysis Started on - java_source	OK
2025-09-01 17:12:04	Android SBOM Analysis Completed	OK
2025-09-01 17:12:09	Android SAST Completed	OK
2025-09-01 17:12:09	Android API Analysis Started	OK
2025-09-01 17:12:13	Android API Analysis Completed	OK

2025-09-01 17:12:13	Android Permission Mapping Started	OK
2025-09-01 17:12:18	Android Permission Mapping Completed	OK
2025-09-01 17:12:18	Android Behaviour Analysis Started	OK
2025-09-01 17:12:23	Android Behaviour Analysis Completed	OK
2025-09-01 17:12:23	Extracting Emails and URLs from Source Code	OK
2025-09-01 17:12:25	Email and URL Extraction Completed	OK
2025-09-01 17:12:25	Extracting String data from APK	OK
2025-09-01 17:12:25	Extracting String data from Code	OK
2025-09-01 17:12:25	Extracting String values and entropies from Code	OK
2025-09-01 17:12:28	Performing Malware check on extracted domains	OK

2025-09-01 17:12:34	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.