MOBSF

ANDROID STATIC ANALYSIS REPORT

Galileo Health (2024.12.20)

File Name:	com.galileohealth.android_33767.apk
Package Name:	com.galileohealth.android
Scan Date:	Aug. 29, 2025, 10:45 p.m.
App Security Score:	50/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	5/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	24	4	4	6

FILE INFORMATION

File Name: com.galileohealth.android_33767.apk
Size: 61.6MB
MD5: 527574f6221d300f6cf61ac1174ee2d2
SHA1: 130bdad33f9d6f2f10de7616c78a8fc5b07319fe
SHA256: 4e95be12b1d98a105f745727c205ae16d324380ef6269d174570c5d7cc5cb696

APP INFORMATION

App Name: Galileo Health
Package Name: com.galileohealth.android
Main Activity: com.galileohealth.android.main.MainActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 2024.12.20

Android Version Code: 33767

APP COMPONENTS

Activities: 57
Services: 17
Receivers: 13
Providers: 4
Exported Activities: 6
Exported Services: 3
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
v2 signature: True
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: 2019-07-29 16:39:27+00:00
Valid To: 2049-07-29 16:39:27+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xaaf6ea9a800394ae65a43fb561be0859abb59e30
Hash Algorithm: sha256
md5: 86cd5f6d705418f4276dfefdeccbf163
sha1: 2e50b618520f0196f7e0deb9292af67a30e33056
sha256: dddbb70541628cab576916a32c73110711f00cd422560bfa67f5c2dfe26ad99b
sha512: 54a5c84b8178ee218c8e382b08be8fcac4a2101cbaefe7ae689a822fe8babf14f60eb7d27a4885d411ca8c96e59bb2fa491296344d4569598d4c1dad609ff88e
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 30c7455d9412f0a91a2fd930543091b9073b24b32cb838b32004042bae1b8399
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	normal	enables foreground services for media playback.	Allows a regular application to use Service.startForeground with the type "mediaPlayback".
android.permission.FOREGROUND_SERVICE_MICROPHONE	normal	permits foreground services with microphone use.	Allows a regular application to use Service.startForeground with the type "microphone".
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.

PERMISSION	STATUS	INFO	DESCRIPTION
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.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
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.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.
com.galileohealth.android.sdk.permission-group.ipc.sender	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.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.galileohealth.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>527574f6221d300f6cf61ac1174ee2d2.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></tr>
</table>

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

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></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.MANUFACTURER check
Build.BOARD check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
<tr><td>classes5.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER 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>classes6.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.BOARD check
SIM operator check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
<tr><td>classes7.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
<tr><td>classes8.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT

ACTIVITY	INTENT
com.galileohealth.android.main.MainActivity	Schemes: galileohealth://, http://, https://, Hosts: app, galileohealth.com, galileo.io, Paths: /open-membership, /dl/open-membership, /reset-password, /dl/reset-password, /prescription, /dl/prescription, /lab-request, /dl/lab-request, /referral, /dl/referral, /medical-consult, /dl/medical-consult, /form, /dl/form, /my-cases, /dl/my-cases, /conversation, /dl/conversation, /doctors, /dl/doctors, /profile, /dl/profile, /phr-wizard, /dl/phr-wizard, /dl/profile-wizard, /profile-wizard, /settings, /dl/settings, /editaccount, /pcp, /dl/pcp, /give-galileo, /dl/give-galileo, /start-ehr-sync, /dl/start-ehr-sync, /ehr-sync-status, /dl/ehr-sync-status, /provider-search, /dl/provider-search, /learn-tab, /dl/learn-tab, /quiz-category, /dl/quiz-category, /dl/form_v2, Path Prefixes: /dl,
com.stripe.android.link.LinkRedirectHandlerActivity	Schemes: link-popup://, Hosts: complete, Paths: /com.galileohealth.android,
com.stripe.android.payments.StripeBrowserProxyReturnActivity	Schemes: stripesdk://, Hosts: payment_return_url, Paths: /com.galileohealth.android,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION

NO	SCOPE	SEVERITY	DESCRIPTION
1	ocsp.digicert.com crl3.digicert.com crl4.digicert.com crl.godaddy.com certificates.godaddy.com crl.starfieldtech.com certificates.starfieldtech.com ocsp.godaddy.com ocsp.starfieldtech.com	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

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

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **13** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	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	TaskAffinity is set for activity (com.zipow.videobox.conference.ui.ZmConfPipActivity)	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.
4	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.
5	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
6	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.
7	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.
8	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.

NO	ISSUE	SEVERITY	DESCRIPTION
9	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.
10	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.
11	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
13	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Activity (androidx.fragment.app.testing.EmptyFragmentActivity) 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.
15	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.

CODE ANALYSIS

HIGH: **2** | WARNING: **9** | INFO: **3** | SECURE: **3** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A/T.java A/W0.java A/e1.java A1/c.java A2/f.java A2/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A4/c.java A4/d.java A4/h.java Aa/C0428a0.java Aa/CallableC0492w0.java Aa/J.java Aa/J1.java Aa/N0.java Aa/P1.java Aa/R1.java Aa/RunnableC0484t0.java Aa/V.java Aa/V0.java Aa/X.java Aa/X0.java Ab/k.java Ab/u.java Ac/b.java Ac/c.java Ac/d.java Ac/g.java Af/AbstractC0519f1.java B/C0600p.java B7/a.java B7/g.java B8/g.java C3/c.java C3/d.java Ca/a.java Ci/e.java Ci/f.java Da/a.java E1/n.java E2/b.java E2/c.java Ed/c.java Eh/a.java F3/c.java F7/n.java Fd/b.java Fh/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				G/f0.java G2/f.java G8/t.java Gb/A.java H1/f.java H2/a.java H5/ViewOnClickListenerC0861p.java Hb/p.java I9/d.java J6/f.java Jb/b.java Jb/e.java Jb/g.java K9/AbstractC1057a.java L9/l.java La/e.java M2/C1163m.java M9/g.java M9/i.java N0/C1258w.java N0/l.java N2/s.java N8/d.java N8/k.java O1/r.java O2/a.java Ob/b.java Ob/e.java Ob/h.java Od/e.java Of/w.java P1/d.java Q/C.java Q/u.java Qb/a.java Qc/d.java Qg/b.java Rb/b.java Rb/c.java Rb/d.java Rj/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				S1/e.java S2/a.java S6/G.java Sb/c.java Sb/d.java T/C1683x.java T9/c.java T9/d.java T9/i.java T9/l.java Tb/b.java U9/b.java U9/d.java U9/e.java U9/f.java U9/i.java U9/j.java U9/k.java U9/l.java U9/m.java U9/n.java Ub/A.java Ub/h.java Ub/j.java Ub/k.java Ub/l.java Ub/n.java Ub/p.java Ub/r.java Ub/s.java Ub/t.java Ub/u.java Ub/v.java Ub/y.java V2/f.java V9/d.java V9/e.java V9/g.java V9/j.java V9/m.java Vb/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	Vb/g.java Vb/m.java W5/p.java Wb/v0.java X8/c.java X9/d.java X9/e.java X9/p.java X9/y.java Xj/m.java Y2/q.java Y9/AbstractC2001e.java Y9/C.java Y9/C2003g.java Y9/D.java Y9/F.java Y9/I.java Y9/K.java Y9/o.java Y9/r.java Yc/h.java Yc/j.java Yc/n.java Yj/d.java Zb/a.java Zb/c.java a1/AbstractC2066E.java ac/C2120c.java b0/C2467r0.java b1/x.java b2/b.java b2/d.java b2/h.java b3/k.java ca/C2660a.java com/adjust/sdk/Logger.java com/braze/support/BrazeLogger.java com/bumptech/glide/b.java com/bumptech/glide/l.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/o.java com/galileohealth/android/account/profile/wizard/ProfileWizardCarouselView.java com/stripe/hcaptcha/webview/HCaptchaWebView.java com/zipow/videobox/ZMFirebaseMessagingService.java com/zipow/videobox/sip/server/CmmSIPNosManager.java com/zipow/videobox/view/sip/feedback/b.java d2/AbstractC2941c.java d4/C2944c.java da/AbstractC2998b.java da/d.java e3/g.java e3/r.java e4/C3056c.java e4/C3057d.java e5/C3059a.java e8/r.java e9/C3117c.java ec/C3122a.java ec/C3123b.java f3/t.java fa/AbstractC3231a.java fb/c.java fh/C3267a.java fl/C3302a.java ha/d.java ha/e.java ha/g.java i4/C3641b.java ib/c.java id/f.java ii/AbstractC3800H.java io/split/android/client/network/b.java j4/C.java j4/i.java j4/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				j4/j.java j4/l.java j4/m.java jb/AbstractC3868a.java k/AbstractC3923o.java k/C3925q.java k/C3931w.java k/LayoutInflaterFactory2C3934z.java k4/C3959f.java k4/C3960g.java kg/f.java l4/C4103f.java la/BinderC4121a.java lb/h.java ll/c.java m/f.java m2/C4177h.java m3/f.java m4/C4180c.java mc/d.java n1/C4275c.java n3/c.java n3/h.java n3/k.java n3/l.java n4/C4281B.java n4/C4287b.java n4/C4289d.java nh/e.java o0/f.java o1/C4380e.java o3/g.java o3/l.java o3/m.java p/h.java p/i.java p1/f.java p4/C4511b.java pc/c.java q/MenuC4625j.java q/ViewOnKeyListenerC4619d.java q2/AbstractC4648a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				q2/AbstractC4648a.java q2/d.java q4/C4653b.java q4/C4654c.java q4/E.java q4/i.java q4/m.java q4/p.java q4/r.java q4/v.java q4/z.java qc/C4679b.java r1/e.java r1/j.java r1/o.java r1/p.java r2/AbstractC4787s.java r2/C4772c.java r2/C4785p.java rc/c.java s1/C4887d.java s1/h.java s1/s.java s1/u.java s1/w.java s1/z.java sd/F.java sf/t.java u/D.java u/G.java u/n.java u/t.java u2/d.java u2/i.java u2/j.java u4/C5191a.java u4/h.java us/zoom/proguard/ea5.java us/zoom/proguard/z6.java us/zoom/zimmsg/a.java va/e.java w4/p.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				w4/p.java w4/q.java wb/C5726d.java wb/C5728f.java y1/AbstractC5904b.java y1/AbstractC5916n.java yc/C5970B.java yc/C5976H.java yc/C5978J.java yc/C5982N.java yc/C5984P.java yc/C5997l.java yc/C5998m.java yc/HandlerC5985Q.java yc/V.java yc/w.java z1/i.java z1/j.java z1/k.java z1/l.java z1/m.java z4/i.java
2	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	Aa/C0451i.java Aa/F0.java Aa/H.java Aa/J1.java Aa/T1.java B7/a.java B7/g.java G2/c.java M2/v.java N8/d.java N8/i.java N8/j.java N8/k.java O8/k.java O8/l.java Yc/l.java Yc/m.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	N0/C1229h.java com/zipow/videobox/conference/ui/dialog/ZmBaseLiveStreamDialog.java com/zipow/videobox/view/sip/coverview/PhonePBXListCoverSummaryView.java com/zipow/videobox/view/sip/voicemail/encryption/ui/b.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/ao1.java us/zoom/unite/jsapi/UniteJsApiRegister.java us/zoom/zmsg/deeplink/DeepLinkViewHelper.java us/zoom/zmsg/richtext/CustomActionModeProvider.java us/zoom/zmsg/view/mm/AbstractViewOnClickListenerC5471f.java
4	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	A2/g.java Aa/P1.java Db/c.java Kb/a.java S8/F.java S8/M.java T8/g.java bo/content/e1.java com/adjust/sdk/Util.java com/braze/support/IntentUtils.java com/zipow/videobox/conference/ui/controller/SymbioticActivityController.java fi/a.java fi/b.java gi/C3495a.java v9/V.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/zipow/videobox/ZoomApplication.java
6	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	Wb/v0.java b2/h.java com/zipow/videobox/MMShareActivity.java com/zipow/videobox/view/sip/sms/ZmPhoneChatInputFragmentBase.java com/zipow/videobox/view/sip/sms/l.java n3/r.java q2/d.java us/zoom/proguard/jh3.java us/zoom/proguard/kr0.java us/zoom/proguard/oz0.java us/zoom/proguard/qx0.java us/zoom/zmsg/fragment/MMChatInputFragment.java us/zoom/zmsg/message/send/processor/FileAndTextProcessor.java us/zoom/zmsg/view/mm/VoiceRecordView.java us/zoom/zmsg/view/mm/VoiceTalkView.java
				Fe/h.java Ne/j.java V7/k.java Y/C1903l1.java Y6/a.java Y6/g.java Y6/j.java b0/Y.java com/adjust/sdk/Constants.java com/braze/configuration/BrazeConfig.java com/galileohealth/android/newpassword/NewPasswordViewState.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/galileohealth/android/payment/api/StripeApiKeyResponse.java com/galileohealth/android/signup/api/InitiateRequest.java com/stripe/android/model/A.java com/stripe/android/model/C2917z.java com/stripe/android/model/ConfirmSetupIntentParams.java com/stripe/android/model/ConsumerSessionSignup.java com/stripe/android/model/ElementsSession.java com/stripe/android/model/PaymentMethodCreateParams.java com/stripe/android/model/Stripe3ds2Fingerprint.java com/stripe/android/payments/core/authentication/threeds2/Stripe3ds2TransactionContract.java com/stripe/android/payments/paymentlauncher/PaymentLauncherContract$Args$IntentConfirmationArgs.java com/stripe/android/payments/paymentlauncher/PaymentLauncherContract$Args$PaymentIntentNextActionArgs.java com/stripe/android/payments/paymentlauncher/PaymentLauncherContract$Args$SetupIntentNextActionArgs.java com/stripe/android/paymentsheet/PaymentSheet$CustomerAccessType$CustomerSession.java com/stripe/android/paymentsheet/PaymentSheet$CustomerAccessType$LegacyCustomerEphemeralKey.java com/stripe/android/paymentsheet/PaymentSheet$CustomerConfiguration.java com/stripe/android/paymentsheet/PaymentSheetContract.java com/stripe/android/paymentsheet/addresselement/AddressElementActivityContract.java com/stripe/android/paymentsheet/addresselement/AddressLauncher$Configuration.java com/stripe/android/paymentsheet/state/Custom

NO	ISSUE	SEVERITY	STANDARDS	FILES
				erState.java com/stripe/android/paymentsheet/state/PaymentElementLoader$InitializationMode$PaymentIntent.java com/stripe/android/paymentsheet/state/PaymentElementLoader$InitializationMode$SetupIntent.java com/stripe/android/stripe3ds2/transaction/AcsData.java com/stripe/android/uicore/elements/AddressType$ShippingCondensed.java com/stripe/android/uicore/elements/AddressType$ShippingExpanded.java com/zipow/videobox/confapp/meeting/reaction/ZmBulletEmojiEmitter.java com/zipow/videobox/ptapp/ZmZRMgr.java com/zipow/videobox/sip/server/CmmSIPCallHistoryItemBean.java ee/q.java h4/C3562h.java io/split/android/client/dtos/KeyImpression.java j4/C3839B.java j4/e.java j4/u.java k8/C3982d.java n3/d.java r9/b.java us/zoom/feature/pbo/ui/ZmPBOUI.java us/zoom/libtools/storage/PreferenceUtil.java us/zoom/libtools/storage/ZmSharePreferenceHelper.java us/zoom/libtools/utils/ZmDeviceUtils.java us/zoom/module/api/sign/model/UserAccount.java us/zoom/module/api/zcalendar/IZCalendarService.java us/zoom/proguard/cq5.java us/zoom/proguard/gf.java us/zoom/proguard/kz4.java us/zoom/zmsg/MMImageListActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	bo/content/SharedPreferencesC2620e.java bo/content/b0.java bo/content/d6.java bo/content/f1.java bo/content/g6.java bo/content/h4.java bo/content/l0.java bo/content/l1.java bo/content/m.java bo/content/m0.java bo/content/m6.java bo/content/n0.java bo/content/r3.java bo/content/v5.java bo/content/w4.java bo/content/y0.java com/braze/configuration/RuntimeAppConfigurationProvider.java com/braze/managers/BrazeGeofenceManager.java us/zoom/asyncview/ViewCacheManager.java
9	This App has capabilities to prevent against Screenshots from Recent Task History/ Now On Tap etc.	secure	OWASP MASVS: MSTG-STORAGE-9	us/zoom/uicommon/activity/ZMActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/zipow/annotate/AnnoUtil.java us/zoom/libtools/utils/ZmDeviceUtils.java us/zoom/proguard/d54.java us/zoom/proguard/ei2.java us/zoom/proguard/iq0.java us/zoom/proguard/mq5.java us/zoom/proguard/n12.java us/zoom/proguard/q83.java us/zoom/proguard/u71.java us/zoom/proguard/vu2.java us/zoom/proguard/yx3.java us/zoom/proguard/zu5.java us/zoom/videomeetings/richtext/ZMRichTextUtil.java us/zoom/zimmsg/chatlist/MMChatsListFragment.java
11	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	Xj/e.java Xj/h.java Xj/l.java Xj/m.java e9/C3117c.java us/zoom/proguard/ym2.java
12	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	ed/AbstractC3128d.java fa/AbstractC3231a.java n3/r.java
13	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	Ub/h.java ub/AbstractC5224b.java us/zoom/proguard/pf5.java wb/C5728f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	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	Aa/P1.java C3/c.java com/braze/support/StringUtils.java us/zoom/proguard/c41.java us/zoom/proguard/i26.java us/zoom/proguard/ym2.java us/zoom/proguard/yx3.java
15	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	hk/InterfaceC3625a.java ik/InterfaceC3834a.java jk/InterfaceC3895a.java kk/InterfaceC4079a.java us/zoom/proguard/oq.java us/zoom/proguard/xt4.java us/zoom/proguard/ym2.java yk/InterfaceC6102e.java
16	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	Ub/h.java bd/e.java qc/C4679b.java rc/c.java
17	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	us/zoom/proguard/n12.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
			Aa/J1.java Aa/P1.java Aa/V0.java Aa/X0.java Af/C0523h.java C6/f.java N0/C1226f0.java Qf/b.java Tf/U.java com/adjust/sdk/ActivityHandler.java com/adjust/sdk/PreinstallUtil.java com/braze/Braze.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java com/stripe/android/link/LinkForegroundActivity.java com/stripe/android/payments/StripeBrowserLauncherActivity.java com/zipow/videobox/JoinByURLActivity.java com/zipow/videobox/JoinMeetingFailActivity.java com/zipow/videobox/LauncherActivity.java com/zipow/videobox/MMShareActivity.java com/zipow/videobox/ZmMainServiceImpl.java com/zipow/videobox/confapp/meeting/confhelper/ZoomRateHelper.java com/zipow/videobox/fragment/AddrBookItemDetailsFragment.java com/zipow/videobox/fragment/DiagnosticsFragment.java com/zipow/videobox/fragment/MyProfileFragment.java com/zipow/videobox/fragment/PermissionGuideFragment.java com/zipow/videobox/fragment/ZmSelectMeetingReminderFragment.java com/zipow/videobox/utils/ZmUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/zipow/videobox/view/sip/sms/PbxSmsTextItemView.java com/zipow/videobox/view/sip/sms/ZmPhoneChatInputFragmentBase.java com/zipow/videobox/widget/MeetingsWidget.java ha/e.java kg/f.java n3/l.java r2/AbstractC4787s.java r2/C4770a.java r2/C4772c.java us/zoom/internal/impl/x.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/a33.java us/zoom/proguard/af4.java us/zoom/proguard/aj.java us/zoom/proguard/aw0.java us/zoom/proguard/bd1.java us/zoom/proguard/ck.java us/zoom/proguard/df3.java us/zoom/proguard/er1.java us/zoom/proguard/h53.java us/zoom/proguard/hm.java us/zoom/proguard/iy4.java us/zoom/proguard/jz0.java us/zoom/proguard/la5.java us/zoom/proguard/ld2.java us/zoom/proguard/ld4.java us/zoom/proguard/lj.java us/zoom/proguard/m64.java us/zoom/proguard/mr0.java us/zoom/proguard/oz5.java us/zoom/proguard/qx0.java us/zoom/proguard/rb2.java us/zoom/proguard/t35.java us/zoom/proguard/tl2.java us/zoom/proguard/uy5.java us/zoom/proguard/v24.java us/zoom/proguard/vz1.java us/zoom/proguard/we1.java us/zoom/proguard/wo3.java us/zoom/proguard/yb2.java us/zoom/proguard/zr.java

RULE ID	BEHAVIOUR	LABEL	FILES
			us/zoom/proguard/zu5.java us/zoom/proguard/zx1.java us/zoom/zapp/fragment/ZappUIComponent.java us/zoom/zapp/misc/BasicModeUIMgr$onClick$3.java us/zoom/zclips/ui/recording/ZClipsRecordingPage.java us/zoom/zimmsg/filecontent/MMSessionFilesFragment.java us/zoom/zimmsg/fragment/IMShareInviteDialog.java us/zoom/zmsg/fragment/MMChatInputFragment.java us/zoom/zmsg/markdown/a.java us/zoom/zmsg/mediaplayer/ZMMediaPlayerActivity.java us/zoom/zmsg/view/mm/AbstractViewOnClickListenerC5471f.java us/zoom/zmsg/view/mm/MMContentFileViewerFragment.java us/zoom/zmsg/view/mm/message/MMMessageRemoveHistory.java us/zoom/zmsg/view/mm/message/MessageRemoveHistoryView.java us/zoom/zmsg/view/mm/message/m0.java v8/ViewOnClickListenerC5540a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	Aa/V0.java Aa/X0.java H4/e.java com/braze/push/BrazeNotificationUtils.java com/stripe/android/link/LinkForegroundActivity.java com/zipow/videobox/IMActivity.java com/zipow/videobox/conference/ui/view/share/ZmBaseShareView.java com/zipow/videobox/fragment/IMAddrBookListFragment.java com/zipow/videobox/fragment/SettingAboutFragment.java h3/c.java id/f.java us/zoom/proguard/ja2.java us/zoom/proguard/sw0.java us/zoom/proguard/wo3.java us/zoom/proguard/yq2.java us/zoom/zimmsg/chats/ShareDocsFragment.java us/zoom/zimmsg/chats/ZmVideoAppContextMenuFragment.java us/zoom/zimmsg/filecontent/MMSessionFilesFragment.java us/zoom/zimmsg/filecontent/a.java us/zoom/zimmsg/reminder/MMRemindersFragment.java us/zoom/zmsg/fragment/MMChatInputFragment.java us/zoom/zmsg/fragment/MMCommonMsgFragment.java us/zoom/zmsg/fragment/a.java us/zoom/zmsg/view/mm/AbstractViewOnClickListenerC5471f.java us/zoom/zmsg/view/mm/MMContentFileViewerFragment.java
00108	Read the input stream from given URL	network command	Aa/C0429a1.java Aa/Q.java J9/v.java e8/r.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	J9/F.java com/adjust/sdk/ActivityHandler.java com/adjust/sdk/DeviceInfo.java com/adjust/sdk/InstallReferrerHuawei.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java com/zipow/videobox/confapp/meeting/confhelper/ZoomRateHelper.java com/zipow/videobox/fragment/ZmSelectMeetingReminderFragment.java com/zipow/videobox/utils/ZmUtils.java com/zipow/videobox/widget/MeetingsWidget.java ha/e.java kg/f.java n3/l.java n4/C4287b.java r2/C4770a.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/AbstractC5389o5.java us/zoom/proguard/aw0.java us/zoom/proguard/df3.java us/zoom/proguard/iy4.java us/zoom/proguard/jz0.java us/zoom/proguard/la5.java us/zoom/proguard/m64.java us/zoom/proguard/q33.java us/zoom/proguard/t35.java us/zoom/proguard/uy5.java us/zoom/proguard/yx3.java us/zoom/proguard/zu5.java
00202	Make a phone call	control	C6/f.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/m64.java

RULE ID	BEHAVIOUR	LABEL	FILES
00203	Put a phone number into an intent	control	C6/f.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/m64.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	C6/f.java Qf/b.java com/stripe/android/link/LinkForegroundActivity.java com/stripe/android/payments/StripeBrowserLauncherActivity.java com/zipow/videobox/ZmMainServiceImpl.java com/zipow/videobox/confapp/meeting/confhelper/ZoomRateHelper.java com/zipow/videobox/fragment/AddrBookItemDetailsFragment.java com/zipow/videobox/fragment/MyProfileFragment.java com/zipow/videobox/view/sip/sms/PbxSmsTextItemView.java com/zipow/videobox/widget/MeetingsWidget.java ha/e.java n3/l.java r2/C4770a.java r2/C4772c.java us/zoom/internal/impl/x.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/aj.java us/zoom/proguard/bd1.java us/zoom/proguard/er1.java us/zoom/proguard/ld4.java us/zoom/proguard/lj.java us/zoom/proguard/m64.java us/zoom/proguard/we1.java us/zoom/proguard/zu5.java us/zoom/zapp/fragment/ZappUIComponent.java us/zoom/zapp/misc/BasicModeUIMgr$onClick$3.java us/zoom/zimmsg/fragment/IMShareInviteDialog.java us/zoom/zmsg/fragment/MMChatInputFragment.java us/zoom/zmsg/view/mm/AbstractViewOnClickListenerC5471f.java us/zoom/zmsg/view/mm/message/m0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	A/N.java C3/d.java Ci/e.java H2/a.java Ph/v.java T1/F.java Vb/g.java Zb/c.java b2/h.java bo/content/v5.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java com/zipow/annotate/AnnoUtil.java com/zipow/cmmlib/AppContext.java com/zipow/videobox/CameraActivity.java com/zipow/videobox/VideoBoxApplication.java com/zipow/videobox/config/ConfigWriter.java com/zipow/videobox/stabilility/StabilityService.java com/zipow/videobox/utils/ZmUtils.java com/zipow/videobox/view/mm/a.java com/zipow/videobox/view/ptvideo/PBXVideoRecordActivity.java ec/C3122a.java q2/d.java s3/k.java s3/n.java tb/W.java tb/k0.java us/zoom/apm/stats/ZMStats.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/AbstractC5389o5.java us/zoom/proguard/bc1.java us/zoom/proguard/bd1.java us/zoom/proguard/d54.java us/zoom/proguard/e32.java us/zoom/proguard/fr5.java us/zoom/proguard/g83.java us/zoom/proguard/i26.java us/zoom/proguard/iq0.java us/zoom/proguard/ja2.java us/zoom/proguard/lh3.java

RULE ID	BEHAVIOUR	LABEL	FILES
			us/zoom/proguard/mq0.java us/zoom/proguard/n44.java us/zoom/proguard/nh3.java us/zoom/proguard/o05.java us/zoom/proguard/om3.java us/zoom/proguard/q83.java us/zoom/proguard/qs0.java us/zoom/proguard/ru0.java us/zoom/proguard/t24.java us/zoom/proguard/tj.java us/zoom/proguard/u71.java us/zoom/proguard/un.java us/zoom/proguard/vq4.java us/zoom/proguard/vu2.java us/zoom/proguard/xv.java us/zoom/proguard/xx3.java us/zoom/proguard/ya1.java us/zoom/proguard/ye2.java us/zoom/proguard/yx3.java us/zoom/proguard/zu5.java us/zoom/zimmsg/chatlist/MMChatsListFragment.java us/zoom/zimmsg/reminder/MMRemindersFragment.java us/zoom/zmsg/fragment/MMChatInputFragment.java us/zoom/zmsg/fragment/a.java us/zoom/zmsg/message/send/processor/FileAndTextProcessor.java us/zoom/zmsg/ptapp/trigger/ZoomMessenger.java us/zoom/zmsg/util/ImagePickHelper.java us/zoom/zmsg/view/mm/AbstractViewOnClickListenerC5471f.java us/zoom/zmsg/view/mm/MMContentFileViewerFragment.java us/zoom/zmsg/view/mm/message/C5492i.java
00009	Put data in cursor to JSON object	file	Yc/l.java Yc/m.java n3/c.java n3/h.java n3/r.java
			A1/c.java A2/c.java A2/f.java A2/m.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	C3/d.java J9/C0980g.java J9/F.java Qc/d.java Qc/f.java Qj/d.java Qj/g.java S2/a.java Sb/d.java T1/A.java T1/F.java Ub/e.java Ub/h.java Ub/p.java V1/e.java Vb/g.java W1/i.java Zb/a.java b2/h.java bo/content/o0.java com/adjust/sdk/PreinstallUtil.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java com/zipow/annotate/ImageUtil.java com/zipow/cmmlib/AppContext.java com/zipow/videobox/VideoBoxApplication.java com/zipow/zm2d/Zm2DImageUtil.java d0/C2936a.java d4/C2944c.java fk/l0.java ii/AbstractC3800H.java j4/l.java n3/r.java n4/C4281B.java s3/k.java tb/C5053B.java tb/C5070q.java tb/C5071s.java tb/M.java tb/U.java

RULE ID	BEHAVIOUR	LABEL	FILES
			tb/X.java tb/d0.java tb/l0.java tb/m0.java tb/r.java us/zoom/apm/stats/ZMStats.java us/zoom/proguard/AbstractC5389o5.java us/zoom/proguard/C5295c4.java us/zoom/proguard/bt1.java us/zoom/proguard/d54.java us/zoom/proguard/fr5.java us/zoom/proguard/ja2.java us/zoom/proguard/jh3.java us/zoom/proguard/lf5.java us/zoom/proguard/lh3.java us/zoom/proguard/mq0.java us/zoom/proguard/nh3.java us/zoom/proguard/q83.java us/zoom/proguard/ru0.java us/zoom/proguard/s23.java us/zoom/proguard/ta.java us/zoom/proguard/tx3.java us/zoom/proguard/vq4.java us/zoom/proguard/wj1.java us/zoom/proguard/xq1.java us/zoom/proguard/xx3.java us/zoom/proguard/yi.java us/zoom/proguard/yx3.java us/zoom/proguard/zf3.java us/zoom/proguard/zm2.java us/zoom/zimmsg/chatlist/MMChatsListFragment.java us/zoom/zimmsg/reminder/MMRemindersFragment.java us/zoom/zmsg/view/ZMFileReaderView.java us/zoom/zmsg/view/mm/AbstractViewOnClickListenerC5471f.java us/zoom/zmsg/view/mm/MMContentFileViewerFragment.java us/zoom/zmsg/view/mm/VoiceTalkRecordView.java z1/k.java z1/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	J9/v.java N8/k.java com/bumptech/glide/load/data/l.java e8/r.java io/split/android/client/network/b.java rc/c.java sf/A.java
00030	Connect to the remote server through the given URL	network	Aa/T.java J9/v.java com/adjust/sdk/AdjustLinkResolution.java com/bumptech/glide/load/data/l.java io/split/android/client/network/b.java lb/e.java sf/A.java
00109	Connect to a URL and get the response code	network command	Aa/RunnableC0484t0.java Aa/T.java He/s.java J9/v.java N8/k.java T9/c.java com/bumptech/glide/load/data/l.java e8/r.java io/split/android/client/network/b.java rc/c.java sf/A.java
00187	Query a URI and check the result	collection sms calllog calendar	us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/f8.java us/zoom/proguard/qq3.java us/zoom/proguard/xw2.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/adjust/sdk/DeviceInfo.java ha/d.java m2/C4172c.java sd/o.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/f8.java us/zoom/proguard/qq3.java us/zoom/proguard/xw2.java us/zoom/proguard/yx3.java
00004	Get filename and put it to JSON object	file collection	Wb/v0.java ec/C3122a.java ha/e.java
00014	Read file into a stream and put it into a JSON object	file	Vb/g.java n3/r.java us/zoom/apm/stats/ZMStats.java
00005	Get absolute path of file and put it to JSON object	file	Vb/g.java ec/C3122a.java us/zoom/apm/stats/ZMStats.java us/zoom/proguard/g83.java
00189	Get the content of a SMS message	sms	com/adjust/sdk/DeviceInfo.java ha/d.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/qq3.java us/zoom/proguard/xw2.java us/zoom/proguard/yx3.java

RULE ID	BEHAVIOUR	LABEL	FILES
00188	Get the address of a SMS message	sms	com/adjust/sdk/DeviceInfo.java ha/d.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/qq3.java us/zoom/proguard/xw2.java us/zoom/proguard/yx3.java
00200	Query data from the contact list	collection contact	com/adjust/sdk/DeviceInfo.java ha/d.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/qq3.java us/zoom/proguard/xw2.java us/zoom/proguard/yx3.java
00201	Query data from the call log	collection calllog	com/adjust/sdk/DeviceInfo.java ha/d.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/qq3.java us/zoom/proguard/xw2.java us/zoom/proguard/yx3.java
00102	Set the phone speaker on	command	com/zipow/videobox/confapp/AudioSessionMgr.java com/zipow/videobox/sip/server/p.java org/webrtc/voiceengine/AudioDeviceAndroid.java org/webrtc/voiceengine/AudioDeviceAndroidAAudio.java org/webrtc/voiceengine/AudioDeviceAndroidOpenSLESHelper.java

RULE ID	BEHAVIOUR	LABEL	FILES
00056	Modify voice volume	control	org/webrtc/voiceengine/AudioDeviceAndroid.java org/webrtc/voiceengine/AudioDeviceAndroidOpenSLESHelper.java us/zoom/proguard/ja2.java us/zoom/proguard/rb3.java us/zoom/proguard/xq1.java us/zoom/zimmsg/reminder/MMRemindersFragment.java us/zoom/zmsg/util/MMAudioMessagePlayer.java us/zoom/zmsg/view/mm/AbstractViewOnClickListenerC5471f.java
00096	Connect to a URL and set request method	command network	J9/v.java N8/k.java e8/r.java io/split/android/client/network/b.java io/split/android/client/network/c.java lb/e.java
00094	Connect to a URL and read data from it	command network	J9/v.java e8/r.java n3/l.java us/zoom/core/model/a.java
00209	Get pixels from the latest rendered image	collection	com/zipow/nydus/camera/CameraCaptureImplV2.java com/zipow/videobox/CameraActivity.java us/zoom/proguard/b22.java us/zoom/proguard/ch5.java
00016	Get location info of the device and put it to JSON object	location collection	Sb/c.java
00079	Hide the current app's icon	evasion	com/zipow/videobox/ptapp/PTUI.java ii/AbstractC3800H.java o3/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	B7/a.java Sb/d.java com/zipow/videobox/CallingActivity.java com/zipow/videobox/VideoBoxApplication.java com/zipow/videobox/ZMFirebaseMessagingService.java com/zipow/videobox/fragment/AddrBookItemDetailsFragment.java com/zipow/videobox/fragment/MyProfileFragment.java com/zipow/videobox/fragment/PermissionGuideFragment.java com/zipow/videobox/ptapp/PTUI.java com/zipow/videobox/view/mm/a.java com/zipow/videobox/view/ptvideo/PBXVideoRecordActivity.java com/zipow/videobox/view/sip/sms/l.java us/zoom/proguard/af4.java us/zoom/proguard/iq0.java us/zoom/proguard/ja2.java us/zoom/proguard/qx0.java us/zoom/proguard/v24.java us/zoom/proguard/vh1.java us/zoom/proguard/xq1.java us/zoom/zimmsg/chatlist/MMChatsListFragment.java us/zoom/zimmsg/chats/session/b.java us/zoom/zmsg/fragment/MMChatInputFragment.java us/zoom/zmsg/ptapp/callback/ZoomBaseMessengerUI.java us/zoom/zmsg/ptapp/trigger/ZoomMessenger.java us/zoom/zmsg/view/mm/AbstractC5467b.java us/zoom/zmsg/view/mm/AbstractViewOnClickListenerC5471f.java us/zoom/zmsg/view/mm/MMContentFileViewerFragment.java
00121	Create a directory	file command	com/zipow/videobox/ZMFirebaseMessagingService.java com/zipow/videobox/view/mm/a.java us/zoom/zimmsg/chatlist/MMChatsListFragment.java us/zoom/zmsg/fragment/MMChatInputFragment.java

RULE ID	BEHAVIOUR	LABEL	FILES
00075	Get location of the device	collection location	k/C3931w.java us/zoom/proguard/ap5.java
00137	Get last known location of the device	location collection	us/zoom/proguard/ap5.java
00065	Get the country code of the SIM card provider	collection	us/zoom/proguard/pr5.java us/zoom/proguard/xr3.java
00132	Query The ISO country code	telephony collection	J9/q.java us/zoom/proguard/xr3.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/xw2.java us/zoom/proguard/yx3.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/adjust/sdk/DeviceInfo.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/xw2.java us/zoom/proguard/yx3.java
00191	Get messages in the SMS inbox	sms	com/adjust/sdk/DeviceInfo.java com/adjust/sdk/InstallReferrerMeta.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/pm1.java us/zoom/proguard/xw2.java us/zoom/proguard/yx3.java
00183	Get current camera parameters and change the setting.	camera	com/zipow/nydus/camera/CameraCaptureImplV1.java com/zipow/nydus/camera/CameraMgrV1.java us/zoom/proguard/n9.java us/zoom/proguard/r9.java

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/zipow/annotate/ImageUtil.java com/zipow/videobox/CameraActivity.java com/zipow/zm2d/Zm2DImageUtil.java us/zoom/proguard/d54.java
00033	Query the IMEI number	collection	bo/content/m0.java com/zipow/videobox/sip/server/CmmSIPCallManager.java us/zoom/libtools/utils/ZmDeviceUtils.java
00083	Query the IMEI number	collection telephony	bo/content/m0.java us/zoom/libtools/utils/ZmDeviceUtils.java
00204	Get the default ringtone	collection	us/zoom/proguard/xv.java us/zoom/proguard/yg4.java
00038	Query the phone number	collection	com/zipow/videobox/sip/server/CmmSIPCallManager.java
00112	Get the date of the calendar event	collection calendar	com/zipow/videobox/view/schedule/ZmScheduleTimeAndRecurringLayout.java us/zoom/proguard/f01.java us/zoom/proguard/h01.java us/zoom/proguard/mt5.java
00162	Create InetSocketAddress object and connecting to it	socket	Xj/c.java Xj/m.java
00163	Create new Socket and connecting to it	socket	Xj/c.java Xj/m.java com/adjust/sdk/network/ActivityPackageSender.java
00208	Capture the contents of the device screen	collection screen	us/zoom/proguard/b22.java us/zoom/proguard/ch5.java

RULE ID	BEHAVIOUR	LABEL	FILES
00104	Check if the given path is directory	file	com/zipow/videobox/VideoBoxApplication.java com/zipow/videobox/fragment/SettingAboutFragment.java us/zoom/zimmsg/chatlist/MMChatsListFragment.java
00028	Read file from assets directory	file	J9/C0975b.java us/zoom/proguard/yq2.java
00026	Method reflection	reflection	Di/j.java wi/z.java
00012	Read data and put it into a buffer stream	file	b2/h.java us/zoom/proguard/C5295c4.java us/zoom/proguard/d54.java us/zoom/proguard/jh3.java us/zoom/proguard/s23.java us/zoom/proguard/yi.java us/zoom/proguard/yx3.java
00175	Get notification manager and cancel notifications	notification	com/zipow/videobox/util/NotificationMgr.java
00024	Write file after Base64 decoding	reflection file	ha/e.java s3/n.java us/zoom/proguard/n12.java
00199	Stop recording and release recording resources	record	us/zoom/proguard/el2.java
00198	Initialize the recorder and start recording	record	us/zoom/proguard/el2.java

RULE ID	BEHAVIOUR	LABEL	FILES
00194	Set the audio source (MIC) and recorded file format	record	us/zoom/proguard/el2.java
00197	Set the audio encoder and initialize the recorder	record	us/zoom/proguard/el2.java
00196	Set the recorded file format and output path	record file	us/zoom/proguard/el2.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	us/zoom/proguard/xt4.java
00130	Get the current WIFI information	wifi collection	us/zoom/proguard/pm3.java us/zoom/proguard/xt4.java
00134	Get the current WiFi IP address	wifi collection	us/zoom/proguard/xt4.java
00082	Get the current WiFi MAC address	collection wifi	us/zoom/proguard/xt4.java
00192	Get messages in the SMS inbox	sms	com/zipow/videobox/fragment/DiagnosticsFragment.java us/zoom/proguard/yx3.java us/zoom/videomeetings/richtext/ZMRichTextUtil.java
00025	Monitor the general action to be performed	reflection	id/f.java
00043	Calculate WiFi signal strength	collection wifi	us/zoom/proguard/pm3.java
00092	Send broadcast	command	us/zoom/proguard/m64.java

RULE ID	BEHAVIOUR	LABEL	FILES
00064	Monitor incoming call status	control	com/zipow/videobox/sip/server/p.java us/zoom/proguard/rb3.java
00002	Open the camera and take picture	camera	com/zipow/nydus/camera/CameraCaptureImplV1.java
00023	Start another application from current application	reflection control	com/zipow/videobox/auto/ZmAutoMeetingScreen$onClickMeet$1.java
00078	Get the network operator name	collection telephony	Yc/f.java bo/content/m0.java
00147	Get the time of current location	collection location	k/C3931w.java
00115	Get last known location of the device	collection location	k/C3931w.java
00114	Create a secure socket connection to the proxy address	network command	Sj/j.java
00123	Save the response to JSON after connecting to the remote server	network command	bo/content/s1.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://galileo-health-production.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/781943603918/namespaces/firebase:fetch?key=AIzaSyDm5AqLEKxhixhfoH21odhz6bV3zsoBQLw. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	7/44	android.permission.CHANGE_NETWORK_STATE, android.permission.FOREGROUND_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BROADCAST_STICKY, android.permission.CALL_PHONE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
ssrv.adjust.cn	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou
subscription.adjust.cn	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou
app.adjust.cn	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou
gdpr.adjust.cn	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
merchant-ui-api.stripe.com	ok	**IP:** 54.187.175.68 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
link.com	ok	**IP:** 35.166.203.173 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
api.stripe.com	ok	**IP:** 52.25.214.31 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
app.adjust.com	ok	**IP:** 185.151.204.8 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
gdpr.adjust.com	ok	**IP:** 185.151.204.51 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
subscription.tr.adjust.com	ok	**IP:** 195.244.54.44 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
ssrv.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
ssrv.adjust.world	ok	**IP:** 185.151.204.206 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
checkout.link.com	ok	**IP:** 18.238.96.79 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
blog.zoom.us	ok	**IP:** 170.114.52.63 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.333698 **Longitude:** -121.889297 **View:** Google Map
www.braze.com	ok	**IP:** 104.17.228.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
link.co	ok	**IP:** 13.224.53.115 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
subscription.adjust.net.in	ok	**IP:** 185.151.204.34 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
firebaseinstallations.googleapis.com	ok	**IP:** 64.233.177.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ssrv.tr.adjust.com	ok	**IP:** 195.244.54.5 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
sdk.split.io	ok	**IP:** 151.101.131.9 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
auth.split.io	ok	**IP:** 44.197.221.236 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
ssrv.adjust.cn	ok	**IP:** 47.104.30.117 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
core-api.prod.galileo.io	ok	**IP:** 54.221.6.35 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
q.stripe.com	ok	**IP:** 54.186.23.98 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
galileo-health-production.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
subscription.adjust.com	ok	**IP:** 185.151.204.52 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
app.adjust.net.in	ok	**IP:** 185.151.204.31 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
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

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
explore.zoom.us	ok	**IP:** 52.84.151.64 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
gdpr.tr.adjust.com	ok	**IP:** 195.244.54.5 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
www.googleadservices.com	ok	**IP:** 74.125.136.157 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
issuetracker.google.com	ok	**IP:** 64.233.177.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ssrv.adjust.com	ok	**IP:** 185.151.204.2 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
gdpr.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
sondheim.braze.com	ok	**IP:** 104.18.43.4 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
subscription.adjust.cn	ok	**IP:** 47.104.30.117 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
telemetry.split.io	ok	**IP:** 3.223.63.250 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.zoom.us	ok	**IP:** 170.114.52.2 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.333698 **Longitude:** -121.889297 **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

DOMAIN	STATUS	GEOLOCATION
developer.apple.com	ok	**IP:** 17.253.83.137 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
app.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
support.zoom.us	ok	**IP:** 170.114.45.6 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.333698 **Longitude:** -121.889297 **View:** Google Map
google.com	ok	**IP:** 142.250.9.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	ok	**IP:** 64.233.176.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app.adjust.cn	ok	**IP:** 47.104.30.117 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
app.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
gdpr.adjust.world	ok	**IP:** 185.151.204.40 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.galileo.io	ok	**IP:** 34.192.41.152 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
subscription.adjust.world	ok	**IP:** 185.151.204.44 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
default.url	ok	No Geolocation information available.
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
notareal.link	ok	No Geolocation information available.
developer.android.com	ok	**IP:** 64.233.176.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 142.251.15.104 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
zoomus.zendesk.com	ok	**IP:** 216.198.53.2 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
streaming.split.io	ok	**IP:** 18.155.173.57 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
subscription.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
app-measurement.com	ok	**IP:** 64.233.177.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
m.stripe.com	ok	**IP:** 34.215.30.129 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
www.example.com	ok	**IP:** 23.56.109.241 **Country:** France **Region:** Provence-Alpes-Cote-d'Azur **City:** Marseille **Latitude:** 43.296951 **Longitude:** 5.381070 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
galileo.helpscoutdocs.com	ok	**IP:** 18.210.189.28 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
app.tr.adjust.com	ok	**IP:** 195.244.54.5 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** Google Map
gdpr.adjust.net.in	ok	**IP:** 185.151.204.32 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
schemas.microsoft.com	ok	**IP:** 13.107.253.71 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
hooks.stripe.com	ok	**IP:** 54.187.175.68 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
www.zoomgov.com	ok	**IP:** 160.1.56.156 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.amazon.com	ok	**IP:** 18.155.172.176 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
zoom.us	ok	**IP:** 170.114.52.2 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.333698 **Longitude:** -121.889297 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
aomedia.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
sdk.iad-01.braze.com	ok	**IP:** 172.64.148.188 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
play.google.com	ok	**IP:** 172.253.124.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebase.google.com	ok	**IP:** 74.125.136.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
twitter.com	ok	**IP:** 162.159.140.229 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
errors.stripe.com	ok	**IP:** 198.202.176.161 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.797550 **Longitude:** -73.946190 **View:** Google Map
ssrv.adjust.net.in	ok	**IP:** 185.151.204.207 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
api.mixpanel.com	ok	**IP:** 107.178.240.159 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
gdpr.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
docs.stripe.com	ok	**IP:** 52.10.212.243 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
gdpr.adjust.cn	ok	**IP:** 47.104.30.117 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
app.adjust.world	ok	**IP:** 185.151.204.42 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
accounts.google.com	ok	**IP:** 142.251.2.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ssrv.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
subscription.us.adjust.com	ok	**IP:** 185.151.204.70 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
galileo.io	ok	**IP:** 54.81.216.181 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
support.stripe.com	ok	**IP:** 198.137.150.161 **Country:** United States of America **Region:** Ohio **City:** Miamisburg **Latitude:** 39.630859 **Longitude:** -84.262108 **View:** Google Map
events.split.io	ok	**IP:** 54.226.96.64 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
stripe.com	ok	**IP:** 52.40.139.248 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 142.250.9.94 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

✉ EMAILS

EMAIL	FILE
support@galileohealth.com	ha/e.java
u0013android@android.com0 u0013android@android.com	V9/i.java
support@stripe.com	e8/r.java
email@me.co	ie/C3716a.java
support@stripe.com	Ld/C1120i.java
email@example.com	ge/C3387b.java
support@stripe.com	Hd/f.java
support@galileohealth.com	com/galileohealth/android/membership/dialogs/IneligibleBottomSheet.java
example@example.com	com/zipow/videobox/view/ABItemDetailsList.java
this@zmsettingfragment.getfragmen	com/zipow/videobox/fragment/settings/ZmSettingFragment.java
support@galileohealth.com user@example.com zdc.pr@zoom.us no-reply@zoom.us support@stripe.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118
Split	Analytics	https://reports.exodus-privacy.eu.org/trackers/349

HARDCODED SECRETS

POSSIBLE SECRETS
"adjust_app_token" : "17uv4npwcyv4"
"adjust_token_registration" : "5q9uvx"
"adjust_token_selected_plan" : "4uc5y1"
"adjust_token_subscriptions" : "l85m7y"
"com.google.firebase.crashlytics.mapping_file_id" : "de4e116fcda24e738fdd4c0d24b6acfb"

POSSIBLE SECRETS
"com_braze_api_key" : "13236bf0-1310-47dc-9248-db947b0f9d87"
"com_braze_firebase_cloud_messaging_sender_id" : "781943603918"
"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"
"firebase_database_url" : "https://galileo-health-production.firebaseio.com"
"google_api_key" : "AIzaSyDm5AqLEKxhixhfoH21odhz6bV3zsoBQLw"
"google_crash_reporting_api_key" : "AIzaSyDm5AqLEKxhixhfoH21odhz6bV3zsoBQLw"
"google_maps_key" : "AIzaSyAJqF_pteWvjwik06uc0e-yzmmQSdoEUDo"
"mixpanel_token" : "5300158e5549f35e5ff371416c62d56f"
"split_api" : "uu3hhhg3snv62d244g7jc9d1nkdefajin9cg"
"stripe_publishable_key" : "pk_live_nj9ZExpzSVI7sJ6zrfSbFuR3"
"twilio_sms_number" : "9179974883"
"zm_deeplink_private_channel_approve_380105" : "Approve"
"zm_deeplink_private_channel_cancel_552125" : "Cancel"

POSSIBLE SECRETS
"zm_deeplink_private_channel_decline_380105" : "Decline"
"zm_facebook_live_key_426839" : "facebook"
"zm_fb_workplace_live_key_426839" : "fb_workplace"
"zm_google_private_meeting_317030" : "Busy"
"zm_im_mention_session_link_552428" : "(#%s)"
"zm_im_session_members_external_393577" : "External"
"zm_im_session_members_external_keywords_393577" : "external"
"zm_mm_call_session_list_format" : "[%s]"
"zm_open_app_feature_shortcut_key_304115" : "feature"
"zm_pbx_private_call_park_brackets_599001" : "(%s)"
"zm_pbx_voicemail_forward_private_330349" : "Private"
"zm_search_authenticate_212554" : "Authenticate"
"zm_sip_sms_session_alert_137657" : "Alert"
"zm_sip_sms_session_member_item_detail_desc_137657" : "Button"
"zm_sip_sms_session_name_other_136896" : "Others"

POSSIBLE SECRETS
"zm_twitch_live_key_426839" : "twitch"
"zm_youtube_live_key" : "youtube"
"zm_zapp_guest_mode_promote_authorize_add_dialog_add_519982" : "Add"
"zoom_api_domain" : "galileo.zoom.us"
"zoom_api_key" : "gr374jJbcI9hkOzHkSHr1Fg5SuslwqVHCQyN"
"zoom_api_secret" : "USdLaiYi02JC1tqFEJna1DLDEjik8wTkberB"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
115792089237316195423570985008687907853269984665640564039457584007908834671663
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
41058363725152142129326129780047268409114441015993725554835256314039467401291
470fa2b4ae81cd56ecbcda9735803434cec591fa
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
2762c874eafb8e94376855402628e842

POSSIBLE SECRETS

dcb428fea25c40e7b99f81ae5981ee6a
3267051002075881697808308513050704318447127338065924327593890433575733 7482424
686479766013060971498190079908139321726943530014330540939446345918554318339765605212255964066145455497729631139148085803712198799971664381257402829111505 7148
109384903807373427451111239076680556993620759895168374899458639449595311615073501601370873757375962324859213229670631330943845253159101291214232748847898 5984
deca87e736574c5c83c07314051fd93a
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
37a6259cc0c1dae299a7866489dff0bd
30820268308201d102044a9c4610300d06092a864886f70d0101040500307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e3020170d3039303833313231353231365a180f32303530303932353231353231365a307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e30819f300d06092a864886f70d010101050003818d0030818902818100c207d51df8eb8c97d93ba0c8c1002c928fab00dc1b42fca5e66e99cc3023ed2d214d822bc59e8e35ddcf5f44c7ae8ade50d7e0c434f500e6c131f4a2834f987fc46406115de2018ebbb0d5a3c261bd97581ccfef76afc7135a6d59e8855ecd7eacc8f8737e794c60a761c536b72b11fac8e603f5da1a2d54aa103b8a13c0dbc10203010001300d06092a864886f70d0101040500038181005ee9be8bcbb250648d3b741290a82a1c9dc2e76a0af2f2228f1d9f9c4007529c446a70175c5a900d5141812866db46be6559e2141616483998211f4a673149fb2232a10d247663b26a9031e15f84bc1c74d141ff98a02d76f85b2c8ab2571b6469b232d8e768a7f7ca04f7abe4a775615916c07940656b58717457b42bd928a2
55066263022277343669578718895168534326250603453777594175500187360389116729240
48439561293906451759052585252797914202762949526041747995844080717082404635286

POSSIBLE SECRETS
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316
85053bf24bba75239b16a601d9387e17
d2d4eb538a47c48f9535c65a94a92a27
115792089237316195423570985008687907852837564279074904382605163141518161494337
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
115792089210356248762697446949407573530086143415290314195533631308867097853951
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846
3071c8717539de5d5353f4c8cd59a032

POSSIBLE SECRETS

7d73d21f1bd82c9e5268b6dcf9fde2cb
686479766013060971498190079908139321726943530014330540939446345918554318339765539424505774633321719753296399637136332111386476861244038034037280889270700 5449
115792089210356248762697446949407573530086143415290314195533631308867097853948
83257109614890299855467512895201081792878530488613155947092059024805031998844192244386437603929473330780865116278 71
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
00a739cb281b1db57bd4de882d8a4543
36134250956749795798585127919587881956611106672985015071877198253568414405109
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
308201e53082014ea00302010202044faa0a6b300d06092a864886f70d01010505003036310b3009060355040613025553312730250603550 40a131e5a6f6f6d20566964656f20436f6d6d756e69636174696f6e7320496e632e3020170d3132303530393036313035315a180f32303632303432373036313035315a3036310b3009060355040613025553312730250603550 40a131e5a6f6f6d20566964656f20436f6d6d756e69636174696f6e7320496e632e30819f300d06092a864886f70d010101050003818d00308189028181009b463f2d26827dcd115aecc70e5124b9d68cd78e401489c9eae4cd19bc4ca0576ad28168a81f71e8d8b5a7cdc956d937510df3cfa956c28d55668894c33ce08052946ae4af1455becfd2243897f1731fd17a547260c5a52daaebf8ab8a9aad1ad18f99ff696dcf7d713f6540f102c274fbfbc895045f25af67d0fe8dedc5365102030100013000d06092a864886f70d0101050500038181000db7990467b840f362bad88c35874abe4d10d3a872356e57581f06fcbac79ebf6d82bb380d14461eded133d9630d77a6b7bcc9953f1ab02437c6317646218b6a37f3c75e833096fa24a473a9b53b1cca4269f0c753ec33239c9a293ea87c27121f424cb9ec1d7765c7fc0c51b7ee2ec4ab9d15a896eeb150ac06fe67086f1c70
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: Galileo: Medical Care

Score: 4.769461 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.galileohealth.android

Developer Details: Galileo Health, Galileo+Health, None, https://galileo.io/, support@galileo.io,

Release Date: Sep 24, 2019 **Privacy Policy:** Privacy link

Description:

Get high-quality medical care in the palm of your hand with Galileo. 24/7 Availability Have a late-night concern or need care over the weekend? We’re here for you around the clock, every day of the year. The Highest-Quality Care, Fast Our providers work as a team to give you the most accurate and effective treatment, every time. Always Within Reach Our easy-to-use app brings the doctor’s office to you - get care by chat, phone, or video. Care For Almost Any Health Need Galileo’s multidisciplinary medical team treats everything from colds to diabetes, saving you expensive specialist visits. What We Can Help With Everyday issues, like: Prescriptions and refills, acne, birth control, hair loss Acute issues, like: Cold and flu, UTIs / STIs, headaches, rashes Chronic conditions, like: Diabetes, hypertension, heart disease, asthma Mental health, like: Anxiety, depression, insomnia

SCAN LOGS

Timestamp	Event	Error
2025-08-29 22:45:53	Generating Hashes	OK
2025-08-29 22:45:54	Extracting APK	OK
2025-08-29 22:45:54	Unzipping	OK

2025-08-29 22:45:55	Parsing APK with androguard	OK
2025-08-29 22:45:55	Extracting APK features using aapt/aapt2	OK
2025-08-29 22:45:56	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 22:46:00	Parsing AndroidManifest.xml	OK
2025-08-29 22:46:01	Extracting Manifest Data	OK
2025-08-29 22:46:01	Manifest Analysis Started	OK
2025-08-29 22:46:01	Reading Network Security config from network_security_config.xml	OK
2025-08-29 22:46:01	Parsing Network Security config	OK
2025-08-29 22:46:01	Performing Static Analysis on: Galileo Health (com.galileohealth.android)	OK
2025-08-29 22:46:01	Fetching Details from Play Store: com.galileohealth.android	OK
2025-08-29 22:46:02	Checking for Malware Permissions	OK

2025-08-29 22:46:02	Fetching icon path	OK
2025-08-29 22:46:02	Library Binary Analysis Started	OK
2025-08-29 22:46:02	Reading Code Signing Certificate	OK
2025-08-29 22:46:03	Running APKiD 2.1.5	OK
2025-08-29 22:46:12	Detecting Trackers	OK
2025-08-29 22:46:18	Decompiling APK to Java with JADX	OK
2025-08-29 22:47:04	Converting DEX to Smali	OK
2025-08-29 22:47:04	Code Analysis Started on - java_source	OK
2025-08-29 22:47:27	Android SBOM Analysis Completed	OK
2025-08-29 22:48:58	Android SAST Completed	OK

2025-08-29 22:48:58	Android API Analysis Started	OK
2025-08-29 22:50:59	Android API Analysis Completed	OK
2025-08-29 22:51:00	Android Permission Mapping Started	OK
2025-08-29 22:53:42	Android Permission Mapping Completed	OK
2025-08-29 22:53:48	Android Behaviour Analysis Started	OK
2025-08-29 22:55:33	Android Behaviour Analysis Completed	OK
2025-08-29 22:55:33	Extracting Emails and URLs from Source Code	OK
2025-08-29 22:56:35	Email and URL Extraction Completed	OK
2025-08-29 22:56:35	Extracting String data from APK	OK
2025-08-29 22:56:36	Extracting String data from Code	OK

2025-08-29 22:56:36	Extracting String values and entropies from Code	OK
2025-08-29 22:56:56	Performing Malware check on extracted domains	OK
2025-08-29 22:57:17	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.