ANDROID STATIC ANALYSIS REPORT

🤖 Blood Sugar (1.6.5)

File Name:	com.blood.sugar.diabetes.tracker_39.apk
Package Name:	com.blood.sugar.diabetes.tracker
Scan Date:	Aug. 29, 2025, 8:10 p.m.
App Security Score:	**45/100 (MEDIUM RISK)**
Grade:	B
Trackers Detection:	9/432

◕ FINDINGS SEVERITY

🐛 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
5	20	3	2	5

📦 FILE INFORMATION

File Name: com.blood.sugar.diabetes.tracker_39.apk
Size: 40.87MB
MD5: 2023dc4a9d859a3c4f97dc44edf2ccd0
SHA1: 60abfe439b474556ec3b564088980468ee8832fd
SHA256: 7ff7e17f6f82e3e464e4738a762dca74c30147b7ba984fa348c74ea41c80671b

ℹ APP INFORMATION

App Name: Blood Sugar
Package Name: com.blood.sugar.diabetes.tracker
Main Activity: com.wavez.bloodsugarpro.splash.LaunchActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 1.6.5

Android Version Code: 39

▣ APP COMPONENTS

Activities: 61
Services: 16
Receivers: 17
Providers: 5
Exported Activities: 1
Exported Services: 2
Exported Receivers: 4
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: 2023-10-16 09:46:23+00:00
Valid To: 2053-10-16 09:46:23+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xda95c47722edd5f47ccd60e8ac9827cac54d71b6
Hash Algorithm: sha256
md5: d167d15176e0ed90c5bbd9ab150d796f
sha1: d67c74cf07280ce990739de9939df1b2f59721f2
sha256: 265535b4a597133c4802672b3abaaf8ae812d329d5e372520411895e7257ec5a
sha512: c7ba47e939fc78aafa08aba2980143b02ea40ea24a495e3d19b732b68e2142b92cc0ce8e01b84585f6ccb6117c0f34f3e80c8ffab175eb16eec2ee376d89be5f
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: a4a4dbfb935db5ebeba6f10b2e27e3d541828cbdb5ebfeeb8f8fd5cf4dc5ccd2
Found 1 unique certificates

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.FOREGROUND_SERVICE_SPECIAL_USE	normal	enables special-use foreground services.	Allows a regular application to use Service.startForeground with the type "specialUse".
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

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.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
com.blood.sugar.diabetes.tracker.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

🔎 APKID ANALYSIS

FILE	DETAILS
2023dc4a9d859a3c4f97dc44edf2ccd0.apk	**FINDINGS** / **DETAILS** Anti-VM Code — possible VM check
classes.dex	**FINDINGS** / **DETAILS** Anti-VM Code — Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check network operator name check Compiler — r8

FILE	DETAILS
classes2.dex	

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check possible VM check
Anti Debug Code	Debug.isDebuggerConnected() check
Compiler	r8 without marker (suspicious)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.blood.sugar.diabetes.tracker,

🔒 NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

📇 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: **8** | INFO: **0** | SUPPRESSED: **0**

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	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Broadcast Receiver (com.wavez.bloodsugarpro.common.services.notifydaily.DailyReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Broadcast Receiver (com.adjust.sdk.AdjustReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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
5	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.
6	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.
7	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
8	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.
9	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: **3** | WARNING: **9** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a/g.java a1/g.java a5/b.java a5/b0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a5/b0.java
				a5/d.java
				a5/j.java
				a5/j0.java
				a5/m.java
				a5/r.java
				a5/t.java
				a5/x.java
				a6/a.java
				ae/c0.java
				ae/h0.java
				ae/o.java
				ae/p.java
				ae/p0.java
				ae/t0.java
				ae/u0.java
				ae/v0.java
				ae/x0.java
				ae/z.java
				ah/e.java
				ai/e2.java
				ai/i1.java
				ai/o2.java
				ai/x2.java
				b0/p.java
				b6/b.java
				ba/a0.java
				ba/j0.java
				ba/q3.java
				ba/z.java
				bb/e.java
				bb/g.java
				bc/d.java
				bc/h.java
				bg/c.java
				bg/f.java
				bg/g.java
				bh/a.java
				bh/e.java
				c0/h.java
				c1/g.java

NO	ISSUE	FILES	SEVERITY	STANDARDS	FILES
					c17i.java
					c2/b.java
					c2/c.java
					c2/g.java
					c5/a.java
					c5/g.java
					c5/j.java
					c9/d.java
					ca/a.java
					ce/d.java
					ce/e.java
					ce/f.java
					ce/j.java
					cg/b.java
					cg/c.java
					cg/e.java
					cg/f.java
					cg/i.java
					cg/k.java
					ci/p.java
					cl/k0.java
					com/adjust/sdk/Logger.java
					com/apm/insight/b/j.java
					com/apm/insight/h/a.java
					com/apm/insight/k/k.java
					com/apm/insight/l/q.java
					com/apm/insight/runtime/o.java
					com/bumptech/glide/b.java
					com/bumptech/glide/c.java
					com/bumptech/glide/d.java
					com/bumptech/glide/l.java
					com/bumptech/glide/load/data/b.java
					com/bumptech/glide/load/data/l.java
					com/bumptech/glide/manager/d.java
					com/bumptech/glide/manager/s.java
					com/bumptech/glide/manager/t.java
					com/bumptech/glide/n.java
					com/bumptech/glide/p.java
					com/bykv/vk/openvk/component/video/pvs/icD/Jd.java
					com/bykv/vk/openvk/component/video/pv

NO	ISSUE	SEVERITY	STANDARDS	FILES
				s/icD/NB.java com/bykv/vk/openvk/component/video/pv s/icD/icD.java
				com/bykv/vk/openvk/component/video/pv s/icD/sUS.java
				com/bykv/vk/openvk/component/video/pv s/icD/yiw.java
				com/bykv/vk/openvk/component/video/pv s/vG/pvs.java
				com/bykv/vk/openvk/preload/falconx/a/a.j ava
				com/bykv/vk/openvk/preload/geckox/logg er/DefaultLogger.java
				com/bytedance/adsdk/lottie/LottieAnimati onView.java
				com/bytedance/adsdk/ugeno/component/i cD.java
				com/bytedance/adsdk/ugeno/component/i mage/RoundImageView.java
				com/bytedance/adsdk/ugeno/component/i mage/pvs.java
				com/bytedance/adsdk/ugeno/core/Wyp.jav a
				com/bytedance/adsdk/ugeno/core/pvs.java
				com/bytedance/adsdk/ugeno/core/so.java
				com/bytedance/adsdk/ugeno/pvs/vG.java
				com/bytedance/sdk/component/NB/icD/pv s.java
				com/bytedance/sdk/component/NB/vG/ic D.java
				com/bytedance/sdk/component/NB/vG/pv s/pvs/icD.java
				com/bytedance/sdk/component/NB/vG/pv s/pvs/pvs.java
				com/bytedance/sdk/component/NB/vG/vG .java
				com/bytedance/sdk/component/adexpress /NB/pvs.java
				com/bytedance/sdk/component/adexpress /pvs/icD/sUS.java
				com/bytedance/sdk/component/embedap

NO	ISSUE	SEVERITY	STANDARDS	FILES
				plog/PangleEncryptUtils.java com/bytedance/sdk/component/embedap plog/PangleEncryptUtilsType4.java com/bytedance/sdk/component/icD.java com/bytedance/sdk/component/pglcrypt/P glCryptUtils.java com/bytedance/sdk/component/so/Jd.java com/bytedance/sdk/component/utils/Hom eWatcherReceiver.java com/bytedance/sdk/component/utils/Ju.jav a com/bytedance/sdk/component/utils/uc.ja va com/bytedance/sdk/component/yiw/Jd/NB .java com/bytedance/sdk/component/yiw/icD/p vs.java com/bytedance/sdk/openadsdk/IP/icD.java com/bytedance/sdk/openadsdk/IP/vG.java com/bytedance/sdk/openadsdk/activity/TT AppOpenAdActivity.java com/bytedance/sdk/openadsdk/api/factory /SDKTypeConfig.java com/bytedance/sdk/openadsdk/api/init/PA GSdk.java com/bytedance/sdk/openadsdk/componen t/icD.java com/bytedance/sdk/openadsdk/componen t/reward/kj.java com/bytedance/sdk/openadsdk/componen t/reward/pvs/IP.java com/bytedance/sdk/openadsdk/componen t/reward/pvs/Mxy.java com/bytedance/sdk/openadsdk/componen t/reward/pvs/bNS.java com/bytedance/sdk/openadsdk/componen t/yiw.java com/bytedance/sdk/openadsdk/core/CvL.j ava com/bytedance/sdk/openadsdk/core/act/p vs.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bytedance/sdk/openadsdk/core/model/PmLdS.java
				com/bytedance/sdk/openadsdk/core/settings/IP.java
				com/bytedance/sdk/openadsdk/core/settings/kj.java
				com/bytedance/sdk/openadsdk/core/settings/mnm.java
				com/bytedance/sdk/openadsdk/core/settings/vG.java
				com/bytedance/sdk/openadsdk/core/widget/NB.java
				com/bytedance/sdk/openadsdk/icD/vG.java
				com/bytedance/sdk/openadsdk/utils/Gp.java
				com/bytedance/sdk/openadsdk/utils/NB.java
				com/bytedance/sdk/openadsdk/utils/jlb.java
				com/bytedance/sdk/openadsdk/utils/zM.java
				com/github/mikephil/charting/charts/PieChart.java
				com/iab/omid/library/bytedance2/utils/d.java
				com/journeyapps/barcodescanner/BarcodeView.java
				com/journeyapps/barcodescanner/CaptureActivity.java
				com/makeramen/roundedimageview/RoundedImageView.java
				com/mbridge/msdk/dycreator/a/a.java
				com/mbridge/msdk/dycreator/baseview/MBScrollView.java
				com/mbridge/msdk/dycreator/baseview/extview/MBExtAcquireRewardPopView.java
				com/mbridge/msdk/dycreator/baseview/extview/MBExtFeedBackView.java
				com/mbridge/msdk/dycreator/baseview/extview/MBExtMBridgeBaitClickView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/mbridge/msdk/dycreator/baseview/eknew/MBExtMBridgeTextView.java
				com/mbridge/msdk/dycreator/bus/BackgroundPoster.java
				com/mbridge/msdk/dycreator/bus/EventBus.java
				com/mbridge/msdk/dycreator/e/g.java
				com/mbridge/msdk/foundation/controller/b.java
				com/mbridge/msdk/foundation/same/report/b/b.java
				com/mbridge/msdk/foundation/same/report/b/d.java
				com/mbridge/msdk/foundation/same/report/d.java
				com/mbridge/msdk/foundation/same/report/l.java
				com/mbridge/msdk/foundation/tools/aa.java
				com/mbridge/msdk/foundation/tools/ad.java
				com/mbridge/msdk/mbnative/controller/NativeController.java
				com/mbridge/msdk/mbnative/controller/d.java
				com/mbridge/msdk/mbnative/e/b.java
				com/mbridge/msdk/newreward/function/a/a/a.java
				com/mbridge/msdk/playercommon/exoplayer2/DefaultRenderersFactory.java
				com/mbridge/msdk/playercommon/exoplayer2/ExoPlayerImpl.java
				com/mbridge/msdk/playercommon/exoplayer2/ExoPlayerImplInternal.java
				com/mbridge/msdk/playercommon/exoplayer2/MediaPeriodHolder.java
				com/mbridge/msdk/playercommon/exoplayer2/SimpleExoPlayer.java
				com/mbridge/msdk/playercommon/exoplayer2/audio/DefaultAudioSink.java
				com/mbridge/msdk/playercommon/exopla

NO	ISSUE	SEVERITY	STANDARDS	FILES
				yer2/drm/ClearKeyUtil.java com/mbridge/msdk/playercommon/exoplayer2/drm/DefaultDrmSession.java com/mbridge/msdk/playercommon/exoplayer2/drm/DefaultDrmSessionManager.java com/mbridge/msdk/playercommon/exoplayer2/extractor/mkv/MatroskaExtractor.java com/mbridge/msdk/playercommon/exoplayer2/extractor/mp3/VbriSeeker.java com/mbridge/msdk/playercommon/exoplayer2/extractor/mp3/XingSeeker.java com/mbridge/msdk/playercommon/exoplayer2/extractor/mp4/AtomParsers.java com/mbridge/msdk/playercommon/exoplayer2/extractor/mp4/FragmentedMp4Extractor.java com/mbridge/msdk/playercommon/exoplayer2/extractor/mp4/MetadataUtil.java com/mbridge/msdk/playercommon/exoplayer2/extractor/mp4/PsshAtomUtil.java com/mbridge/msdk/playercommon/exoplayer2/extractor/mp4/TrackEncryptionBox.java com/mbridge/msdk/playercommon/exoplayer2/extractor/ogg/VorbisUtil.java com/mbridge/msdk/playercommon/exoplayer2/extractor/ts/AdtsReader.java com/mbridge/msdk/playercommon/exoplayer2/extractor/ts/Id3Reader.java com/mbridge/msdk/playercommon/exoplayer2/extractor/ts/PesReader.java com/mbridge/msdk/playercommon/exoplayer2/extractor/wav/WavHeaderReader.java com/mbridge/msdk/playercommon/exoplayer2/mediacodec/MediaCodecInfo.java com/mbridge/msdk/playercommon/exoplayer2/mediacodec/MediaCodecRenderer.java com/mbridge/msdk/playercommon/exoplayer2/mediacodec/MediaCodecUtil.java com/mbridge/msdk/playercommon/exopla

NO	ISSUE	SEVERITY	STANDARDS	FILES
				yer2/metadata/id3/Id3Decoder.java com/mbridge/msdk/playercommon/exoplayer2/offline/DownloadManager.java
				com/mbridge/msdk/playercommon/exoplayer2/offline/DownloadService.java com/mbridge/msdk/playercommon/exoplayer2/source/chunk/BaseMediaChunkOutput.java com/mbridge/msdk/playercommon/exoplayer2/source/chunk/ChunkSampleStream.java com/mbridge/msdk/playercommon/exoplayer2/source/chunk/ChunkedTrackBlacklistUtil.java com/mbridge/msdk/playercommon/exoplayer2/text/cea/Cea708Decoder.java com/mbridge/msdk/playercommon/exoplayer2/text/cea/CeaUtil.java com/mbridge/msdk/playercommon/exoplayer2/text/dvb/DvbParser.java com/mbridge/msdk/playercommon/exoplayer2/text/subrip/SubripDecoder.java com/mbridge/msdk/playercommon/exoplayer2/text/ttml/TtmlDecoder.java com/mbridge/msdk/playercommon/exoplayer2/text/webvtt/WebvttCue.java com/mbridge/msdk/playercommon/exoplayer2/text/webvtt/WebvttCueParser.java com/mbridge/msdk/playercommon/exoplayer2/upstream/DefaultDataSource.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/mbridge/msdk/playercommon/exoplayer2/upstream/DefaultHttpDataSource.java com/mbridge/msdk/playercommon/exoplayer2/upstream/Loader.java com/mbridge/msdk/playercommon/exoplayer2/upstream/cache/CachedRegionTracker.java com/mbridge/msdk/playercommon/exoplayer2/upstream/cache/SimpleCache.java com/mbridge/msdk/playercommon/exoplayer2/util/AtomicFile.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/mbridge/msdk/playercommon/exoplayer2/util/EventLogger.java
				com/mbridge/msdk/playercommon/exoplayer2/util/Util.java
				com/mbridge/msdk/playercommon/exoplayer2/video/DummySurface.java
				com/mbridge/msdk/playercommon/exoplayer2/video/MediaCodecVideoRenderer.java
				com/mbridge/msdk/tracker/b.java
				com/mbridge/msdk/tracker/c.java
				com/mbridge/msdk/tracker/j.java
				com/mbridge/msdk/tracker/k.java
				com/mbridge/msdk/tracker/m.java
				com/mbridge/msdk/tracker/n.java
				com/mbridge/msdk/tracker/network/ae.java
				com/mbridge/msdk/tracker/p.java
				com/mbridge/msdk/tracker/r.java
				com/mbridge/msdk/tracker/w.java
				com/mbridge/msdk/tracker/y.java
				com/mbridge/msdk/video/module/MBridgeBaseView.java
				com/mbridge/msdk/widget/FeedbackRadioGroup.java
				com/wavez/bloodsugarpro/App.java
				com/wavez/bloodsugarpro/MainActivity.java
				com/wavez/bloodsugarpro/bloodsugar/viewmodels/AddBloodSugarViewModel.java
				com/wavez/bloodsugarpro/bloodsugar/viewmodels/BloodSugarViewModel.java
				com/wavez/bloodsugarpro/bmi/viewmodels/TrackViewBmiModel.java
				com/wavez/bloodsugarpro/common/baseapp/ads/appopen/AppOpenManager.java
				com/wavez/bloodsugarpro/info/activities/InfoDetailActivity.java
				com/wavez/bloodsugarpro/stress/viewmodels/MeasurementViewModel.java
				d/d.java
				d3/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				d3/p.java
				d9/e.java
				d9/f.java
				d9/j.java
				d9/k.java
				d9/p.java
				d9/t.java
				d9/w.java
				db/f.java
				db/k.java
				db/m.java
				dc/c.java
				dh/d.java
				dh/h.java
				e2/a.java
				e2/d.java
				e6/b0.java
				e6/e0.java
				e6/f0.java
				e6/o0.java
				e6/q0.java
				e7/a.java
				ea/a.java
				ec/d.java
				eg/c.java
				el/e.java
				f/c.java
				f/c0.java
				f/d0.java
				f/f.java
				f/h0.java
				f/l.java
				f/s.java
				f/v.java
				f1/p.java
				f5/i.java
				f9/e0.java
				f9/f.java
				f9/h.java
				f9/u.java
				fg/a.java

NO	ISSUE		SEVERITY	STANDARDS	FILES
					fg/d.java
					fi/f.java
					g1/j.java
					g1/k.java
					g1/l.java
					g1/m.java
					g1/n.java
					g1/r.java
					g5/g.java
					g7/g.java
					g9/e.java
					g9/g0.java
					g9/h.java
					g9/h0.java
					g9/j0.java
					g9/m0.java
					g9/q.java
					g9/t.java
					g9/w.java
					h0/c.java
					h1/c.java
					h4/c.java
					ha/b.java
					i/i.java
					i/j.java
					i0/f.java
					i0/k.java
					i0/r.java
					i7/a.java
					i7/b.java
					i7/c.java
					i7/f.java
					i7/g.java
					j/i.java
					j/o.java
					j1/o.java
					j2/b.java
					j2/e.java
					j7/b.java
					j7/c.java
					j7/e.java
					j9/a.java

NO	ISSUE		SEVERITY	STANDARDS	FILES
					j9/a.java
					jb/b.java
					jb/d.java
					jb/g.java
					jd/m.java
					jd/n.java
					jg/f.java
					k/e1.java
					k/f2.java
					k/i1.java
					k/i3.java
					k/k.java
					k/k2.java
					k/l2.java
					k/m0.java
					k/o2.java
					k/s0.java
					k/u2.java
					k/y.java
					k0/a.java
					k1/a.java
					k2/b.java
					k3/g.java
					k3/o.java
					k4/b.java
					k5/b.java
					k9/c.java
					kb/l.java
					kb/n.java
					kg/h.java
					l1/e.java
					l7/c.java
					l7/d.java
					l9/a.java
					ld/m.java
					lg/b.java
					ll/r.java
					ll/w.java
					m2/a.java
					m6/b.java
					m7/a.java

NO	ISSUE		SEVERITY	STANDARDS	FILES
					m77b.java
					m7/d.java
					m7/e.java
					m7/g.java
					m7/i.java
					m7/k.java
					m8/h0.java
					me/l.java
					n1/b.java
					n1/j0.java
					n1/j1.java
					n1/o.java
					n1/r1.java
					n1/s1.java
					n1/v0.java
					n1/w1.java
					n1/z0.java
					n2/d.java
					n4/a.java
					n6/a0.java
					n6/x.java
					n8/h.java
					n9/e.java
					n9/g.java
					nk/h1.java
					oh/i.java
					p4/c.java
					p4/d.java
					p5/b.java
					p5/d0.java
					p5/r0.java
					p5/t.java
					p5/u.java
					pa/c.java
					pd/c.java
					pi/d.java
					pi/e.java
					pi/f.java
					pi/g.java
					pj/f.java
					q4/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				q4/e.java
				q5/e.java
				q5/h.java
				q5/m.java
				q5/w.java
				q7/p.java
				qd/b.java
				qd/d.java
				r/a0.java
				r/e0.java
				r/i.java
				r/j0.java
				r2/d.java
				r3/e.java
				rd/c.java
				ri/c.java
				rj/g.java
				s2/c1.java
				s2/n0.java
				s2/x.java
				s4/c.java
				se/c.java
				se/d.java
				sj/f0.java
				t0/d.java
				t1/r.java
				t2/a0.java
				t2/m.java
				t2/o.java
				t2/q.java
				t2/r.java
				t2/s.java
				t2/z.java
				t4/h0.java
				t4/l.java
				t4/m.java
				t4/p.java
				t4/z.java
				t5/j.java
				t5/k.java
				t8/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t9/e.java
				t9/f.java
				t9/h.java
				t9/l.java
				te/a.java
				u3/f.java
				u4/g.java
				u4/h.java
				u5/g.java
				ub/e.java
				ub/g.java
				uf/h.java
				v0/e.java
				v1/e.java
				v4/i.java
				vd/a.java
				w1/s.java
				w5/b.java
				w5/c.java
				w6/a.java
				w6/b.java
				w7/c.java
				w7/i.java
				wd/b.java
				wd/d.java
				wd/h.java
				wd/l.java
				wj/j.java
				x2/c.java
				x4/f.java
				x4/h.java
				x4/n.java
				y/a1.java
				y/d.java
				y/r0.java
				y0/c.java
				y0/f.java
				y0/g.java
				y0/j.java
				y0/n.java
				y2/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				y5/e.java y5/i.java y5/j.java y5/k.java y6/l.java y9/c0.java y9/e.java y9/g.java y9/g0.java y9/o.java y9/v.java y9/y0.java ya/d.java yc/e.java yg/e.java yg/o.java z/i.java z/n.java z2/a.java z4/b.java z5/h.java z9/g.java za/a.java zg/a.java zg/c.java zg/g.java zh/i.java zq/i.java
				com/adjust/sdk/Constants.java com/bykv/vk/openvk/component/video/pvs/icD/Mxy.java com/mbridge/msdk/MBridgeConstans.java com/mbridge/msdk/foundation/download/core/DownloadCommon.java com/mbridge/msdk/foundation/download/core/DownloaderReporter.java com/mbridge/msdk/foundation/entity/CampaignEx.java com/mbridge/msdk/newreward/player/MB

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	RewardVideoActivity.java com/mbridge/msdk/newreward/player/imodel/IBigTempModel.java com/mbridge/msdk/newreward/player/imodel/IECModel.java com/mbridge/msdk/newreward/player/imodel/IMoreOfferModel.java com/mbridge/msdk/newreward/player/imodel/IPlayModel.java com/mbridge/msdk/newreward/player/iview/IBaseWebView.java com/mbridge/msdk/newreward/player/iview/IMetaData.java com/mbridge/msdk/newreward/player/iview/IPlayTempleView.java com/mbridge/msdk/newreward/player/model/BigTemplateModel.java com/mbridge/msdk/newreward/player/model/ECTempleModel.java com/mbridge/msdk/newreward/player/model/MoreOfferModel.java com/mbridge/msdk/newreward/player/model/PlayTempleModel.java com/mbridge/msdk/newreward/player/model/WebTemplateModel.java com/mbridge/msdk/newreward/player/model/WebViewECModel.java com/mbridge/msdk/newreward/player/view/WebViewTemplate.java com/mbridge/msdk/newreward/player/view/ectemplate/WebViewEC.java com/mbridge/msdk/playercommon/exoplayer2/drm/DefaultDrmSessionManager.java com/mbridge/msdk/video/dynview/moffer/MOfferModel.java dm/k.java o/b.java r4/k.java s5/j.java t4/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t4/f0.java f4/x.java ap/a.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	aq/a.java aq/b.java bp/a.java com/bytedance/sdk/openadsdk/BuildConfig.java cp/a.java cq/e.java dp/a.java ep/a.java fp/a.java hp/a.java ip/c.java ip/i.java jp/a.java l7/c.java lg/b.java mp/a.java so/a.java to/a.java uo/a.java vo/a.java xo/a.java yo/a.java zo/a.java
4	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	dh/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	ba/x3.java com/apm/insight/l/v.java com/bykv/vk/openvk/component/video/api/sUS/icD.java com/bykv/vk/openvk/preload/geckox/utils/g.java com/bytedance/sdk/component/NB/vG/vG/vG.java com/bytedance/sdk/component/utils/NB.java com/mbridge/msdk/foundation/download/core/OkHTTPFileDownloadTask.java com/mbridge/msdk/foundation/download/resource/MBResourceManager.java com/mbridge/msdk/foundation/tools/aa.java com/pgl/ssdk/C0163q.java h4/c.java j8/o.java y5/k.java y9/c0.java yc/e.java
6	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	b0/f.java com/pgl/ssdk/C0163q.java com/pgl/ssdk/ces/c.java dh/c.java hc/h.java jb/b.java k9/c.java ld/i.java qd/b.java
				b0/f.java ba/x3.java bc/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				cm/b4.java cm/f4.java cm/g1.java
7	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	cm/v2.java com/adjust/sdk/Util.java com/apm/insight/i.java com/bytedance/sdk/component/sUS/pvs/sUS/vG.java com/bytedance/sdk/component/utils/pvs.java com/bytedance/sdk/component/yiw/vG/sUS.java com/bytedance/sdk/openadsdk/core/model/OT.java com/bytedance/sdk/openadsdk/icD/qh.java com/bytedance/sdk/openadsdk/utils/jlb.java com/mbridge/msdk/dycreator/baseview/rewardpopview/MBAcquireRewardPopView.java com/mbridge/msdk/playercommon/exoplayer2/source/ShuffleOrder.java com/mbridge/msdk/playercommon/exoplayer2/trackselection/RandomTrackSelection.java com/mbridge/msdk/playercommon/exoplayer2/upstream/cache/CachedContentIndex.java com/mbridge/msdk/thrid/okhttp/OkHttpClient.java com/mbridge/msdk/thrid/okhttp/internal/ws/RealWebSocket.java com/mbridge/msdk/thrid/okhttp/internal/ws/WebSocketWriter.java dm/n.java e2/a.java fl/b.java j8/o.java jm/v.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				mc/c.java hb/E.java p5/n.java
				tn/a.java tn/b.java un/a.java vd/h.java vd/i.java wd/b.java wd/g.java
8	[This App may have root detection capabilities.](#)	secure	OWASP MASVS: MSTG-RESILIENCE-1	wd/l.java com/apm/insight/nativecrash/c.java com/bytedance/sdk/openadsdk/icD/pvs/vG.java com/bytedance/sdk/openadsdk/utils/jlb.java hc/h.java jb/g.java
9	[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](#)	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	ba/a4.java ba/h0.java ba/j.java ba/q3.java com/apm/insight/e/b/a.java com/apm/insight/e/b/b.java com/bykv/vk/openvk/component/video/pvs/icD/icD/Jd.java com/bykv/vk/openvk/preload/geckox/a/b.java com/bytedance/sdk/component/sUS/pvs/pvs/pvs/Jd.java com/bytedance/sdk/component/sUS/pvs/pvs/pvs/icD.java com/bytedance/sdk/openadsdk/core/sUS.java com/bytedance/sdk/openadsdk/mnm/icD.java com/mbridge/msdk/foundation/db/BatchReportDao.java com/mbridge/msdk/foundation/db/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
	Information should be encrypted and written to the database.		OWASP Top 10: M7: Client Code Quality	com/mbridge/msdk/foundation/db/c.java com/mbridge/msdk/foundation/db/e.java com/mbridge/msdk/foundation/db/g.java
				com/mbridge/msdk/foundation/download/ database/DatabaseHelper.java com/mbridge/msdk/newreward/function/d /c.java com/mbridge/msdk/tracker/b.java i0/f.java q5/m.java r/c2.java r/i.java r/m.java w7/c.java w7/h.java w7/i.java x7/h.java x7/n.java y2/c.java
10	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/bytedance/sdk/component/adexpress /NB/NB.java com/bytedance/sdk/component/widget/SS WebView.java
11	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/bytedance/sdk/openadsdk/common/ Wyp.java
12	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	bk/b.java c6/b.java no/m.java p5/m0.java p5/r0.java w5/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
13	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/mbridge/msdk/mbbid/common/b.java
14	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/mbridge/msdk/thrid/okhttp/internal/Util.java
15	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	cl/o.java cl/q.java com/apm/insight/entity/d.java com/apm/insight/l/w.java com/apm/insight/nativecrash/c.java com/bytedance/sdk/openadsdk/utils/jlb.java com/mbridge/msdk/foundation/same/report/b/d.java com/mbridge/msdk/foundation/tools/ag.java com/pgl/ssdk/ces/c.java e6/l0.java
16	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/mbridge/msdk/playercommon/exoplayer2/util/Util.java qd/d.java t9/e.java
17	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	com/bytedance/sdk/component/Jd/pvs.java dh/d.java

👤 NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

🔗 BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
			ai/a2.java ai/b3.java ai/h2.java ai/k2.java ai/y.java c0/b.java ci/t.java cl/x.java com/apm/insight/b/b.java com/apm/insight/g/a.java com/apm/insight/h/b.java com/apm/insight/h/c.java com/apm/insight/k/b.java com/apm/insight/l/f.java com/apm/insight/l/i.java com/apm/insight/l/o.java com/apm/insight/nativecrash/NativeImpl.java com/apm/insight/nativecrash/a.java com/apm/insight/nativecrash/b.java com/apm/insight/nativecrash/c.java com/apm/insight/nativecrash/d.java com/apm/insight/runtime/h.java com/apm/insight/runtime/k.java com/apm/insight/runtime/s.java

RULE ID	BEHAVIOUR	LABEL	FILES
			com/bykv/vk/openvk/component/video/api/vG.java
			com/bykv/vk/openvk/component/video/pvs/Jd/Jd.java
			com/bykv/vk/openvk/component/video/pvs/icD/pvs/vG.java
			com/bykv/vk/openvk/component/video/pvs/pvs/pvs/pvs.java
00022	Open a file from given absolute path of the file	file	com/bykv/vk/openvk/preload/falconx/loader/a.java
			com/bykv/vk/openvk/preload/geckox/a/a/e.java
			com/bykv/vk/openvk/preload/geckox/a/c.java
			com/bykv/vk/openvk/preload/geckox/buffer/a/a.java
			com/bykv/vk/openvk/preload/geckox/buffer/a/b.java
			com/bykv/vk/openvk/preload/geckox/buffer/a/c.java
			com/bykv/vk/openvk/preload/geckox/d/a/a/c.java
			com/bykv/vk/openvk/preload/geckox/d/a/b/d.java
			com/bykv/vk/openvk/preload/geckox/d/a/b/e.java
			com/bykv/vk/openvk/preload/geckox/d/b/a/c.java
			com/bykv/vk/openvk/preload/geckox/d/b/a/d.java
			com/bykv/vk/openvk/preload/geckox/d/b/b/e.java
			com/bykv/vk/openvk/preload/geckox/d/b/b/f.java
			com/bykv/vk/openvk/preload/geckox/d/c.java
			com/bykv/vk/openvk/preload/geckox/f/a.java
			com/bykv/vk/openvk/preload/geckox/f/a/c.java
			com/bykv/vk/openvk/preload/geckox/f/b.java
			com/bykv/vk/openvk/preload/geckox/g/c.java
			com/bykv/vk/openvk/preload/geckox/utils/BsPatch.java
			com/bykv/vk/openvk/preload/geckox/utils/c.java
			com/bytedance/adsdk/lottie/Jd/so.java
			com/bytedance/adsdk/lottie/Jd/yiw.java
			com/bytedance/adsdk/lottie/yiw.java
			com/bytedance/sdk/component/adexpress/pvs/icD/vG.java
			com/bytedance/sdk/component/icD.java
			com/bytedance/sdk/component/utils/sUS.java
			com/bytedance/sdk/openadsdk/CacheDirFactory.java
			com/bytedance/sdk/openadsdk/component/reward/Jd.java
			com/bytedance/sdk/openadsdk/component/reward/qh.java
			com/bytedance/sdk/openadsdk/component/sUS.java
			com/bytedance/sdk/openadsdk/component/yiw/pvs.java
			com/bytedance/sdk/openadsdk/core/settings/bNS.java
			com/bytedance/sdk/openadsdk/core/video/icD/pvs.java
			com/bytedance/sdk/openadsdk/icD/Jd/pvs/pvs.java
			com/bytedance/sdk/openadsdk/multipro/vG.java
			com/mbridge/msdk/foundation/download/resource/MBResourceManager.java
			com/mbridge/msdk/foundation/download/utils/Objects.java

RULE ID	BEHAVIOUR	LABEL	FILES
			com/mbridge/msdk/foundation/same/b/e.java
			com/mbridge/msdk/foundation/tools/ag.java
			com/mbridge/msdk/foundation/tools/ah.java
			com/mbridge/msdk/mbbanner/common/c/b.java
			com/mbridge/msdk/newreward/function/c/c/w.java
			com/mbridge/msdk/newreward/function/command/receiver/a/h.java
			com/mbridge/msdk/newreward/function/command/receiver/a/i.java
			com/mbridge/msdk/newreward/player/presenter/PlayTemplePresenter.java
			com/mbridge/msdk/newreward/player/presenter/PlayWebPresenter.java
			com/mbridge/msdk/reward/adapter/c.java
			com/mbridge/msdk/splash/c/d.java
			com/mbridge/msdk/video/module/a/a/o.java
			com/pgl/ssdk/B.java
			com/pgl/ssdk/K.java
			h4/d.java
			ic/h.java
			qc/a.java
			t9/e.java
			w1/a0.java
			w1/m0.java
			y3/k.java
			y3/n.java

RULE ID	BEHAVIOUR	LABEL	FILES
00005	Get absolute path of file and put it to JSON object	file	com/apm/insight/b/b.java com/apm/insight/k/b.java com/apm/insight/l/i.java com/apm/insight/nativecrash/b.java com/apm/insight/nativecrash/c.java com/apm/insight/runtime/s.java com/bytedance/sdk/openadsdk/component/reward/Jd.java com/bytedance/sdk/openadsdk/component/reward/qh.java com/bytedance/sdk/openadsdk/component/sUS.java com/bytedance/sdk/openadsdk/component/yiw/pvs.java com/bytedance/sdk/openadsdk/core/video/icD/pvs.java com/bytedance/sdk/openadsdk/icD/Jd/pvs/pvs.java com/mbridge/msdk/newreward/player/presenter/PlayWebPresenter.java com/mbridge/msdk/reward/adapter/c.java com/pgl/ssdk/K.java ic/h.java qc/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	com/apm/insight/b/b.java com/apm/insight/entity/b.java com/apm/insight/k/b.java com/apm/insight/k/d.java com/apm/insight/k/e.java com/apm/insight/l/i.java com/apm/insight/l/v.java com/apm/insight/nativecrash/b.java com/apm/insight/nativecrash/c.java com/apm/insight/runtime/s.java com/bytedance/sdk/openadsdk/Wyp/vG.java com/bytedance/sdk/openadsdk/component/reward/Jd.java com/bytedance/sdk/openadsdk/component/reward/qh.java com/bytedance/sdk/openadsdk/component/sUS.java com/bytedance/sdk/openadsdk/core/settings/mnm.java com/bytedance/sdk/openadsdk/core/settings/vG.java com/bytedance/sdk/openadsdk/core/video/icD/pvs.java com/mbridge/msdk/foundation/tools/ab.java com/pgl/ssdk/C0163q.java com/pgl/ssdk/y.java q5/m.java qc/a.java qd/d.java y/d.java z5/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	c6/a.java com/apm/insight/l/a.java com/apm/insight/l/i.java com/bytedance/sdk/openadsdk/core/video/icD/pvs.java com/mbridge/msdk/foundation/tools/ab.java com/mbridge/msdk/foundation/tools/ai.java com/mbridge/msdk/newreward/function/h/c.java com/pgl/ssdk/C0163q.java ic/h.java m4/e.java nc/b.java qd/d.java r/i.java y/x.java y9/g0.java
			c1/i.java c2/g.java c6/a.java cl/v.java com/adjust/sdk/PreinstallUtil.java com/apm/insight/k/j.java com/apm/insight/l/a.java com/apm/insight/l/d.java com/apm/insight/l/i.java com/bykv/vk/openvk/component/video/pvs/Jd/Jd.java com/bykv/vk/openvk/preload/geckox/f/a/c.java com/bytedance/adsdk/lottie/Jd/so.java com/bytedance/adsdk/lottie/Jd/yiw.java com/bytedance/sdk/component/NB/vG/pvs/pvs/pvs.java com/bytedance/sdk/component/adexpress/pvs/icD/icD.java com/bytedance/sdk/component/adexpress/pvs/icD/so.java com/bytedance/sdk/component/icD.java com/bytedance/sdk/component/utils/NB.java com/bytedance/sdk/component/utils/sUS.java

RULE ID	BEHAVIOUR	LABEL	FILES
			com/bytedance/sdk/openadsdk/core/settings/bNS.java com/bytedance/sdk/openadsdk/core/video/icD/pvs.java com/bytedance/sdk/openadsdk/utils/dX.java com/mbridge/msdk/dycreator/a/a.java
00013	Read file and put it into a stream	file	com/mbridge/msdk/foundation/tools/ab.java com/mbridge/msdk/foundation/tools/ai.java com/mbridge/msdk/newreward/function/h/c.java com/mbridge/msdk/playercommon/exoplayer2/upstream/ContentDataSource.java com/mbridge/msdk/playercommon/exoplayer2/upstream/RawResourceDataSource.java com/mbridge/msdk/playercommon/exoplayer2/util/AtomicFile.java com/mbridge/msdk/thrid/okio/Okio.java com/pgl/ssdk/C0163q.java g1/l.java g1/m.java h1/c.java h4/d.java hc/e.java hc/h.java hc/n.java ic/h.java jh/g.java lc/a.java m4/e.java nc/b.java p4/d.java p4/f.java p5/t.java q5/g.java qd/d.java r/i.java r2/a.java r2/d.java r2/i.java sh/u.java t2/y.java w1/h0.java w1/m0.java y/x.java

RULE ID	BEHAVIOUR	LABEL	FILES
			y1/f.java y3/f.java y3/k.java y5/k.java
			y9/g0.java z1/k.java
00096	Connect to a URL and set request method	command network	zq/i.java ba/a0.java com/apm/insight/k/e.java com/apm/insight/k/j.java com/bumptech/glide/manager/d.java com/bytedance/adsdk/lottie/Jd/icD.java com/bytedance/sdk/component/NB/icD/pvs.java com/bytedance/sdk/component/icD/pvs/pvs/pvs/icD.java com/bytedance/sdk/openadsdk/IP/vG.java com/mbridge/msdk/click/h.java com/mbridge/msdk/newreward/player/redirect/UrlReDirectController.java com/mbridge/msdk/playercommon/exoplayer2/upstream/DefaultHttpDataSource.java com/mbridge/msdk/tracker/network/toolbox/h.java com/pgl/ssdk/G.java r/i.java y9/d1.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	ba/k2.java ba/q0.java c9/d.java com/apm/insight/k/e.java com/apm/insight/k/j.java com/bumptech/glide/load/data/l.java com/bumptech/glide/manager/d.java com/bytedance/sdk/component/icD/pvs/pvs/pvs/icD.java com/bytedance/sdk/openadsdk/IP/vG.java com/mbridge/msdk/click/h.java com/mbridge/msdk/foundation/download/download/DownLoadUtils.java com/mbridge/msdk/newreward/player/redirect/UrlReDirectController.java com/mbridge/msdk/playercommon/exoplayer2/upstream/DefaultHttpDataSource.java com/mbridge/msdk/tracker/network/toolbox/h.java com/pgl/ssdk/G.java n8/k.java r/i.java rd/c.java y9/d1.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/apm/insight/k/e.java com/apm/insight/k/j.java com/bumptech/glide/load/data/l.java com/bumptech/glide/manager/d.java com/bytedance/sdk/component/NB/icD/pvs.java com/bytedance/sdk/openadsdk/IP/vG.java com/mbridge/msdk/click/h.java com/mbridge/msdk/foundation/download/download/DownLoadUtils.java com/mbridge/msdk/playercommon/exoplayer2/upstream/DefaultHttpDataSource.java com/mbridge/msdk/tracker/network/toolbox/h.java com/pgl/ssdk/G.java m6/b.java r/i.java rd/c.java y9/d1.java
00030	Connect to the remote server through the given URL	network	ba/a0.java ba/q0.java com/adjust/sdk/AdjustLinkResolution.java com/bumptech/glide/load/data/l.java com/bytedance/adsdk/lottie/Jd/icD.java com/bytedance/sdk/component/NB/icD/pvs.java com/bytedance/sdk/component/icD/pvs/pvs/pvs/icD.java com/mbridge/msdk/click/h.java com/mbridge/msdk/playercommon/exoplayer2/upstream/DefaultHttpDataSource.java com/pgl/ssdk/G.java

RULE ID	BEHAVIOUR	LABEL	FILES
00094	Connect to a URL and read data from it	command network	com/apm/insight/k/e.java com/apm/insight/k/j.java com/bytedance/sdk/component/NB/icD/pvs.java com/mbridge/msdk/foundation/download/download/DownLoadUtils.java com/mbridge/msdk/playercommon/exoplayer2/upstream/DefaultHttpDataSource.java com/pgl/ssdk/G.java k5/b.java
00108	Read the input stream from given URL	network command	ba/j2.java ba/o0.java com/apm/insight/k/e.java com/apm/insight/k/j.java com/bytedance/sdk/component/NB/icD/pvs.java com/bytedance/sdk/component/icD/pvs/pvs/pvs/so.java com/mbridge/msdk/foundation/download/download/DownLoadUtils.java com/mbridge/msdk/playercommon/exoplayer2/upstream/DefaultHttpDataSource.java com/pgl/ssdk/G.java
			al/c.java ba/q3.java ba/x3.java bb/e.java bd/a.java cl/n0.java cl/x.java com/adjust/sdk/ActivityHandler.java com/adjust/sdk/PreinstallUtil.java com/bytedance/sdk/openadsdk/activity/TTWebsiteActivity.java com/bytedance/sdk/openadsdk/common/Mxy.java com/bytedance/sdk/openadsdk/core/act/pvs.java com/bytedance/sdk/openadsdk/core/ae.java com/bytedance/sdk/openadsdk/core/widget/pvs/NB.java com/bytedance/sdk/openadsdk/qh/vG.java

RULE ID	BEHAVIOUR	LABEL	FILES
			com/bytedance/sdk/openadsdk/utils/DeviceUtils.java
			com/bytedance/sdk/openadsdk/utils/cR.java
			com/bytedance/sdk/openadsdk/utils/jlb.java
			com/com/bytedance/overseas/sdk/pvs/icD.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/com/bytedance/overseas/sdk/pvs/pvs.java
			com/karumi/dexter/listener/SettingsClickListener.java
			com/mbridge/msdk/activity/DomainMBCommonActivity.java
			com/mbridge/msdk/click/c.java
			com/mbridge/msdk/foundation/tools/MIMManager.java
			com/mbridge/msdk/foundation/tools/ah.java
			com/mbridge/msdk/foundation/webview/a.java
			com/mbridge/msdk/mbbanner/common/communication/BannerExpandDialog.java
			com/mbridge/msdk/mbbanner/common/communication/a.java
			com/mbridge/msdk/mbbanner/view/a.java
			com/mbridge/msdk/mbsignalcommon/commonwebview/CommonWebView.java
			com/mbridge/msdk/newreward/player/model/BaseWebContentModel.java
			com/mbridge/msdk/splash/signal/SplashExpandDialog.java
			com/mbridge/msdk/video/module/a/a/a.java
			d9/f.java
			e6/f0.java
			e6/l0.java
			e6/o0.java
			e6/q0.java
			ik/x.java
			jg/l.java
			jg/m.java
			jg/n.java
			k/k.java
			n6/b.java
			nk/a3.java
			qk/s.java
			w1/s.java
			y9/v.java
			z5/c.java
00003	Put the compressed bitmap data into JSON object	camera	y9/q.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	ao/z.java cl/n0.java com/adjust/sdk/ActivityHandler.java com/adjust/sdk/DeviceInfo.java com/adjust/sdk/InstallReferrerHuawei.java com/bytedance/sdk/openadsdk/core/ae.java com/bytedance/sdk/openadsdk/utils/cR.java com/bytedance/sdk/openadsdk/utils/jlb.java com/com/bytedance/overseas/sdk/pvs/icD.java com/karumi/dexter/listener/SettingsClickListener.java com/mbridge/msdk/foundation/tools/MIMManager.java com/mbridge/msdk/foundation/tools/ai.java com/mbridge/msdk/mbbanner/common/c/b.java com/mbridge/msdk/splash/c/e.java d9/f.java e6/l0.java e6/w0.java ik/x.java x4/n.java z5/c.java
00034	Query the current data network type	collection network	com/apm/insight/l/p.java com/bykv/vk/openvk/preload/geckox/utils/h.java com/mbridge/msdk/foundation/tools/z.java z5/c.java
00012	Read data and put it into a buffer stream	file	c2/g.java q5/g.java y5/k.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	com/mbridge/msdk/mbbanner/common/communication/a.java com/mbridge/msdk/reward/adapter/c.java com/mbridge/msdk/splash/c/e.java r/i.java z5/a.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	bb/e.java com/bytedance/sdk/openadsdk/activity/TTWebsiteActivity.java com/bytedance/sdk/openadsdk/common/Mxy.java com/bytedance/sdk/openadsdk/core/ae.java com/bytedance/sdk/openadsdk/core/widget/pvs/NB.java com/bytedance/sdk/openadsdk/qh/vG.java com/bytedance/sdk/openadsdk/utils/cR.java com/com/bytedance/overseas/sdk/pvs/icD.java com/com/bytedance/overseas/sdk/pvs/pvs.java com/mbridge/msdk/click/c.java com/mbridge/msdk/foundation/tools/ah.java com/mbridge/msdk/video/module/a/a/a.java d9/f.java e6/l0.java e6/q0.java ik/x.java jg/l.java jg/m.java jg/n.java z5/c.java
00191	Get messages in the SMS inbox	sms	com/adjust/sdk/DeviceInfo.java com/adjust/sdk/InstallReferrerMeta.java com/bytedance/sdk/openadsdk/multipro/pvs/pvs.java com/mbridge/msdk/foundation/tools/MIMManager.java e6/f0.java z5/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	com/adjust/sdk/network/ActivityPackageSender.java com/mbridge/msdk/thrid/okhttp/OkHttpClient.java com/mbridge/msdk/thrid/okhttp/internal/connection/StreamAllocation.java com/mbridge/msdk/thrid/okhttp/internal/platform/AndroidPlatform.java com/mbridge/msdk/thrid/okhttp/internal/platform/Platform.java
00009	Put data in cursor to JSON object	file	com/mbridge/msdk/foundation/db/c.java com/mbridge/msdk/foundation/db/k.java com/mbridge/msdk/foundation/tools/MIMManager.java com/mbridge/msdk/newreward/function/d/a.java q5/m.java t9/l.java y/d.java z5/c.java
00091	Retrieve data from broadcast	collection	com/mbridge/msdk/foundation/tools/MIMManager.java e6/f0.java m4/t.java m8/n0.java n3/b.java n6/c0.java u3/f.java
00104	Check if the given path is directory	file	y9/c0.java
00024	Write file after Base64 decoding	reflection file	com/bytedance/adsdk/lottie/yiw.java y3/n.java
00015	Put buffer stream (data) to JSON object	file	e6/l0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00078	Get the network operator name	collection telephony	com/apm/insight/entity/Header.java e6/l0.java
00028	Read file from assets directory	file	com/mbridge/msdk/playercommon/exoplayer2/upstream/AssetDataSource.java
00189	Get the content of a SMS message	sms	com/adjust/sdk/DeviceInfo.java e6/f0.java n9/e.java
00188	Get the address of a SMS message	sms	com/adjust/sdk/DeviceInfo.java e6/f0.java n9/e.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/adjust/sdk/DeviceInfo.java e6/f0.java
00200	Query data from the contact list	collection contact	com/adjust/sdk/DeviceInfo.java e6/f0.java n9/e.java
00187	Query a URI and check the result	collection sms calllog calendar	e6/f0.java
00201	Query data from the call log	collection calllog	com/adjust/sdk/DeviceInfo.java e6/f0.java n9/e.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/adjust/sdk/DeviceInfo.java e6/f0.java f/v.java n9/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/bytedance/sdk/component/utils/Jd.java t9/e.java
00162	Create InetSocketAddress object and connecting to it	socket	com/mbridge/msdk/thrid/okhttp/internal/platform/AndroidPlatform.java com/mbridge/msdk/thrid/okhttp/internal/platform/Platform.java
00123	Save the response to JSON after connecting to the remote server	network command	ba/a0.java
00153	Send binary data over HTTP	http	com/apm/insight/k/e.java com/mbridge/msdk/tracker/network/toolbox/h.java
00075	Get location of the device	collection location	f/c.java
00137	Get last known location of the device	location collection	f/c.java
00183	Get current camera parameters and change the setting.	camera	cg/f.java

🗄 FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/963490987497/namespaces/firebase:fetch?key=AIzaSyCxOBq8maxdzNz2DHDvRlNRhE81-yrdSUU is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'advice_inter_rewarded': 'false', 'advice_reward': 'true', 'hidden_native_ads': 'false', 'inter_ads_gap': '60000', 'inter_and_open_app_gap': '7000', 'is_monetization': 'false', 'main_banner': 'true', 'max_time_gap': '30000', 'min_time_gap': '5000', 'native_language': 'true', 'noti_status': '1', 'number_ignore_gap_request_ad': '2', 'number_native_ad_need_load': '1', 'tracker_banner': 'true', 'tracker_native': 'true', 'user': 'false'}, 'state': 'UPDATE', 'templateVersion': '45'}

⠿ ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.CAMERA, android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	3/44	android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, 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
app.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
gdpr.adjust.cn	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou
ssrv.adjust.cn	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou

⚲ DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
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
ssdk-va.pangle.io	ok	**IP:** 96.16.55.147 **Country:** United States of America **Region:** Louisiana **City:** New Orleans **Latitude:** 29.954651 **Longitude:** -90.075073 **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
gdpr.tr.adjust.com	ok	**IP:** 195.244.54.6 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** [Google Map](#)
www.googleadservices.com	ok	**IP:** 74.125.136.156 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
graph-video.s	ok	No Geolocation information available.
app.adjust.net.in	ok	**IP:** 185.151.204.30 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** [Google Map](#)
whatwg.org	ok	**IP:** 165.227.248.76 **Country:** United States of America **Region:** New Jersey **City:** Clifton **Latitude:** 40.858429 **Longitude:** -74.163757 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
support.google.com	ok	**IP:** 64.233.177.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app.adjust.com	ok	**IP:** 185.151.204.12 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
issuetracker.google.com	ok	**IP:** 64.233.177.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
gdpr.adjust.com	ok	**IP:** 185.151.204.50 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
subscription.tr.adjust.com	ok	**IP:** 195.244.54.5 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** [Google Map](#)
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](#)
fundingchoicesmessages.google.com	ok	**IP:** 64.233.176.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
play.google.com	ok	**IP:** 172.253.124.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
graph.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api16-access-sg.pangle.io	ok	**IP:** 23.62.226.175 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
googlemobileadssdk.page.link	ok	**IP:** 74.125.21.132 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
github.com	ok	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
log.sgsnssdk.com	ok	**IP:** 23.45.173.146 **Country:** United States of America **Region:** California **City:** El Segundo **Latitude:** 33.919182 **Longitude:** -118.416473 **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
firebase.google.com	ok	**IP:** 74.125.136.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sites.google.com	ok	**IP:** 142.250.9.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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](#)
developer.android.com	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](#)
www.google.com	ok	**IP:** 142.251.15.147 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
sf16-fe-tos-sg.i18n-pglstatp.com	ok	**IP:** 23.32.152.242 **Country:** United States of America **Region:** Florida **City:** West Palm Beach **Latitude:** 26.715340 **Longitude:** -80.053368 **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
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
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

DOMAIN	STATUS	GEOLOCATION
ssdk-sg.pangle.io	ok	**IP:** 96.16.55.157 **Country:** United States of America **Region:** Louisiana **City:** New Orleans **Latitude:** 29.954651 **Longitude:** -90.075073 **View:** Google Map
developers.facebook.com	ok	**IP:** 31.13.70.1 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
subscription.eu.adjust.com	ok	**IP:** 185.151.204.60 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
sf16-static.i18n-pglstatp.com	ok	**IP:** 23.220.73.53 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map
app-measurement.com	ok	**IP:** 64.233.177.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pangolin16.sgsnssdk.com	ok	**IP:** 23.66.3.72 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.363598 **Longitude:** -71.085205 **View:** Google Map
api16-endcard-pack-sg.pangle.io	ok	**IP:** 23.62.226.170 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.example.com	ok	**IP:** 23.220.73.58 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map
subscription.adjust.cn	ok	**IP:** 47.104.30.117 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
subscription.adjust.net.in	ok	**IP:** 185.151.204.34 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
pangolin16.isnssdk.com	ok	**IP:** 23.62.226.163 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
gdpr.adjust.cn	ok	**IP:** 47.104.30.117 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
firebaseremoteconfigrealtime.googleapis.com	ok	**IP:** 172.217.215.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sf19-static.i18n-pglstatp.com	ok	**IP:** 151.101.198.73 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
app.adjust.world	ok	**IP:** 185.151.204.41 **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:** 172.217.215.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sf16-scmcdn-sg.ibytedtos.com	ok	**IP:** 23.206.229.173 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **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
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

DOMAIN	STATUS	GEOLOCATION
log-mva.isnssdk.com	ok	**IP:** 23.62.226.165 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** [Google Map](#)
gist.github.com	ok	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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](#)
app.tr.adjust.com	ok	**IP:** 195.244.54.6 **Country:** Turkey **Region:** Izmir **City:** Izmir **Latitude:** 38.412731 **Longitude:** 27.138380 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
gdpr.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
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
ns.adobe.com	ok	No Geolocation information available.
ssrv.adjust.cn	ok	**IP:** 47.104.30.117 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
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
www.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
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
schemas.android.com	ok	No Geolocation information available.
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
www.pangleglobal.com	ok	**IP:** 23.62.226.171 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.googletagmanager.com	ok	**IP:** 74.125.21.97 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
p16-sign-sg.tiktokcdn.com	ok	**IP:** 23.32.152.247 **Country:** United States of America **Region:** Florida **City:** West Palm Beach **Latitude:** 26.715340 **Longitude:** -80.053368 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	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
.facebook.com	ok	No Geolocation information available.

✉ EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	d9/r.java
dreamcity.techvn@gmail.com	w1/s.java

🕵 TRACKERS

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

TRACKER	CATEGORIES	URL
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
IAB Open Measurement	Advertisement, Identification	https://reports.exodus-privacy.eu.org/trackers/328
Mintegral	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/200
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "993c7e6c8d8844318e70ee8a4072dce2"
"dyStrategy.privateAddress" : "privateAddress"
"facebook_client_token" : "c6087c48af11a93cb61be7cc978bfe42"
"google_api_key" : "AIzaSyCxOBq8maxdzNz2DHDvRlNRhE81-yrdSUU"
"google_crash_reporting_api_key" : "AIzaSyCxOBq8maxdzNz2DHDvRlNRhE81-yrdSUU"

POSSIBLE SECRETS

"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"

"com_facebook_device_auth_instructions" : "facebook.com/device􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀"

"com_facebook_device_auth_instructions" : "􀀀􀀀facebook.com/device􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀"

9douHjmTTjq3N4YYUdzzHaKyxIqsB5K92p8t26vKQB1HahpVak+32YHan4LmgLPE

h7KsLkfPW+xUhoPBD+QqJk2MWrfXYN==

LdxThdi1WBKUL75ULBPBD+QqJk2MWrfXYN==

V8P78mWO+MxnWR283vMX+BSDXEvrm8XlQCYXMpvUe5w=

49f946663a8deb7054212b8adda248c6

3fysZeGzwX+hqd2f4+qtlSho+oF+DeFl9kzKrTFOSWo=

c56fb7d591ba6704df047fd98f535372fea00211

h7KsLkfPW+xUhoPwJ7JgY7K0DkeAWrfXYN==

8a3c4b262d721acd49a4bf97d5213199c86fa2b9

36864200e0eaf5284d884a0e77d31646

Rx5KxmHu63h8QT7T4cYR2mu7F4LQnYkocG/Azb9HP8ZHyjUHnRxxCuB99BIp3kbl

9b8f518b086098de3d77736f9458a3d2f6f95a37

POSSIBLE SECRETS

cca47107bfcbdb211d88f3385aeede40

QcEEfK1PwFv2Eb+NZQ+4kWKAUUVvycYqoBzmAjBexJV/sKEjaFlajeD5MAZYWXy5

JAIugkcNQRXP51pRzjbhWzeihtmzLSCJCmT0+GTbkts=

Y7c14Z2TDbv/Y+xgHFeXDrcshBPUYFT=

DkPtYdQTLkfAW+xUhoPwJ7JgY7K0DkeAWrfXYN==

2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3

avDZD6/xoSbFYvWCy23XLncB75oD5DxKdrTKFY2O0hY=

Kx8fghNUQq+sA+EfmK6qh0KjuKvw753ECuaCFV8szVM=

t+CAjrsoEFEWDgC/oCfdqxFl31lIReQPqb6CaFb+1Y0=

6JHAw9/xzu8LcH4q9f7Udi9sTntehS9dfukXhX8DEHhp54WYBhd6ZhWkqnOAMGmY

fHaUCxrr3fcbpdQPVJw6OSoHeHoizr6wmxmAsnLvDUhuNG2u8ebKX4VPxAoXSx4W

a0784d7a4716f3feb4f64e7f4b39bf04

u7Ufq5yuXkEXg69T8jpWuOOX55Q9g2DSVI1gtbNUvY8=

ngqbGKXcQCvq0ft27xRzOzNoEVN+ei+Vq2+CNx9QQMc=

bFK3lRg0oaTUwYDrSsMiLa/j4LG9nRlI5KKEyt63x08=

POSSIBLE SECRETS

8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f

a4008fff6a22ff9e82cac5fe69bd0388

eUrWQVF8FAlcOLX3Auj55rxdEWjF+0P5JAPLCHVKKQw=

258EAFA5-E914-47DA-95CA-C5AB0DC85B11

vvYcBqgl4aoC3GZZ7n1bdLp71k52s6EJLh0/nA6ME39LmvOZf3TBZ+H4xg1YfQXg

l4qa5EABhdRHJHltXD4U8dy0wNZl4oyoZ9TbFONnMI4=

ZdMwT5n8r4APV4u4GhQlb1VCwOIVHkTm7kF7LnArEpyZnsv+C3G3q6fVFgtTcqcc

af60eb711bd85bc1e4d3e0a462e074eea428a8

5kY1EQ+6snGNdZX1BEywItRy0EAwZ4DbRiPucqHAgfZR8kr75HzXIMEIf0cE9z11

0njjbCFUq6vJ1UgnErUI7KEtLgZLN7V9IJ5yZ3QtzXmjMaTjzKInpeDNakYTgh0P

DFKwWgtuDkKwLZPwD+z8H+N/xjQZxVfV+T2SZVe6V2xS5c5n

HkzwDFeD4QuyLdx5igfZYcu9xTM9NN==

KvkOAoIl09ZSAixqGUOtipMDBdKXVlslzVnQOpfDZOEJW+xbFKrK173Gu3h1RVkI

POSSIBLE SECRETS

30820268308201d102044a9c4610300d06092a864886f70d0101040500307a310b30090603550406130255533310b3009060355040813024341311230100060355040713 0950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b0603550403131446616 365626f6f6b20436f72706f726174696f6e3020170d3039303833313231353231365a180f3230353030393235323131353231365a307a310b30090603550406130255533310b 3009060355040813024341311230100060355040713095061c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b13084 6616365626f6f6b311d301b0603550403131446616365626f6f6b20436f72706f726174696f6e30819f300d06092a864886f70d010101050003818d0030818902818100c2 07d51df8eb8c97d93ba0c8c1002c928fab00dc1b42fca5e66e99cc3023ed2d214d822bc59e8e35ddcf5f44c7ae8ade50d7e0c434f500e6c131f4a2834f987fc46406115de20 18ebbb0d5a3c261bd97581ccfef76afc7135a6d59e8855ecd7eacc8f8737e794c60a761c536b72b11fac8e603f5da1a2d54aa103b8a13c0dbc10203010001300d06092a864 886f70d0101040500038181005ee9be8bcbb250648d3b741290a82a1c9dc2e76a0af2f2228f1d9f9c4007529c446a70175c5a900d5141812866db46be6559e2141616483 998211f4a673149fb2232a10d247663b26a9031e15f84bc1c74d141ff98a02d76f85b2c8ab2571b6469b232d8e768a7f7ca04f7abe4a775615916c07940656b58717457b4 2bd928a2

92762936dcbdd57fe235fd7cf61c2e93da3c4

SKSJAjN3UKeguXyEasCGg04d/yJuUN8XZYgactMp4rfMtHcIJcD0mydl5RKvI49M

cc2751449a350f668590264ed76692694a80308a

tnRfJM39LV6MDlXml8e8fAfi5JhKcsRyFSmagsP97rbE/0XgA5fRVLlLbAYUcu57

FLgp79R6LGLnWDio6G1XBjsjORgKSjLkdakyn5bigQludVyQtVZMhDAlppvakfKf

0781feb2-bf4b-4ff8-be68-9149e288a420

bae8e37fc83441b16034566b

DFKwWgtuDkKwLZPwD+z8H+N/xjK+n3eyNVx6ZVPn5jcincKZx5f5ncN=

O+vmm8flr2e7ZrTWUx/T8ClWwcEwLlJlfjM8sMGjZbg=

83d508d01db531b4cf4843d2e41348ed

TvLSh+Eka5RyCXMK4lvAvP4vfksx/KqJwxjzSKu7qQs=

POSSIBLE SECRETS

Kq6mcF8LH4HqXGyg5/DR3VvLtDExNTPXoCRIPhkdOGM=

470fa2b4ae81cd56ecbcda9735803434cec591fa

AMztxBQmasdCMrU1nlH2RhtlfSPsjcYFxTHFmKvCDYM=

a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc

GC4CZUnPsyUcm5NrWw7C8gSktjb/gtBCDrSKBLlqImuOnQy7zHyo6XlIzkH3EMVH

LdxThdi1WBKUL75ULBPwJ7JgY7K0DkeAWrfXYN==

gYgEHbtWs2qrOou4Pi9x8/evNQKl7xufkAwk8FBwpKpll2nmAbj5wvKo77J2SETY

DFKwWgtuDkKwLZPwD+z8H+N/xj26Vjcdx5KyVj5GxVN=

XThCVgADKYpdOEJWAAMpijdExKKDLYCp1GNXWw

fd71964ced204df586b63b9d8fa3198a

94952e1b52dce00af06084c97b52db3f

8E4cUkgIY9w8/0qt+Oeyh9wfu9tQKpeKsR+Ou+hsYewuB4uFdKW1FI4W+bAZwe0B

6jGSPrUM0+2YrTO2vsTOKq3+XL/IfUFs5oxZaSEvsQg=

DFKwWgtuDkKwLZPwD+z8H+N/xj26Vjcdx5KanjKnxVN=

WfvM4SeNDVyFarUKUVpVTE2MRQkjnaN4GpgwC5lMrmyQkCennlTSSkgCAZvzOVXK

POSSIBLE SECRETS

df6b721c8b4d3b6eb44c861d4415007e5a35fc95

K/sgHSTVeE1LLZ4HP+m5KF6ND+k7W4ID3M3VTul8bAI=

DkP3hrKuHoPMH+zwL+fALkK/WQc5x5zH+TcincKNNVfWNVJcVM==

0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78

DFK/HrQgJ+zQW+xUhoPwJ7JgY7K0DkeAWrfXYN==

9ObkV+9nuY0gPBNLH25GoxM7YATuF1pi7IORvVFb3+Q=

eb321fa50173a95c041b0389a565b006

5HcA415u1KU8m2yVlDZBhQQK+0IFNRmmWPxuAq0DnfPzSdJ/uWlnYMD1kKfkH6cZ

NtWyZSC7qBNyKPaXbOjRpNaZGUUAwpDpvYkB4v1ZH9M=

0yxvRSsGg+/BBPRqwe1F54W0T+vv1NRnE+jebtT36Vo=

M2RhhRYJhjrQUa7n9jg23IBcTQvCkUFLA/9ZbQYvHFo=

iz9pI8M74OdFMOjBXhk6CVKK/c29GtinDT3TfbuphLdYOSnoV+Rg8WuW9whaa7rD

DFK/HrQgJ+zQW+xUhoPBD+QqJk2MWrfXYN==

POSSIBLE SECRETS

308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a4361
6c69666f726e69613116301406035504071307130d4d6f756e7461696e20566696577311143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64
726f6964311030300e06035504031307416e64726f6964301e170d30383030383231323333313333345a170d33363030313037323333313333345a3074310b30090603550406130255
5533113301106035504081308130a43616c69666f726e69613116301406035504071307130d4d6f756e7461696e20566696577311143012060355040a130b476f6f676c6520496e632
e3110300e060355040b1307416e64726f6964311030300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010
0100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a4
3b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764
cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db89
99552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04
160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b30
09060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307130d4d6f756e7461696e20566696577311143012060355040a130b476
f6f676c6520496e632e3110300e060355040b1307416e64726f6964311030300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030
101ff300d06092a864886f70d0101040500038201010006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce607
63b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f60
09ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb62
7ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308
a

6B110692F5A44A1D9905357FBD634283

LYoHKR17UvbUNibqKPKJklawQJNaw1zk7CnhZAC68YBTzC7x4MYQVXp9Sihs98Ok

80818283848586878889 8a8b8c8d8e8f909192939495969798999a9b9c9d9e9f

B3EEABB8EE11C2BE770B684D95219ECB

SHfJbyMgI7MrHewwYoTmYsM7CTkziBSZ0pvzhPCRWcLGoNw6AaEZWLqlKa0dpKuD

d7YRusR2mxxBt1bBYjK2gXVvJl/MfqFw2IiZZVeFOFqksQBErGXLOKgf56kYtWpK

g3h/WBQ8k1SqFyNwcX6aXlyabMyZPKS0QgL4qcVfix1XI+70++CdiHkDZKRlUPQw

lnMUlT0qopStslq/RfZHkyvg0xAUTVuMPsMot4SEaYA=

POSSIBLE SECRETS

936dcbdd57fe235fd7cf61c2e93da3c4

c103703e120ae8cc73c9248622f3cd1e

SkMlFTLt8H3eQLYvgf87g2pXBfp4xPpxL3RMs974XSU=

DFeuWkH0W+xUhoPwJ7JgY7K0DkeAWrfXYN==

308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d0101040500308194310b3009060355040613025553311330110603550408130a436
16c69666f726e69613116301406035504071307130d4d6f756e7461696e20566965577311030300e060355040a1307416e64726f69643110300e060355040b1307416e64726f696
43110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d30383803431353233333
635365a170d33353303930313233333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307130d4
d6f756e7461696e20566965577311030300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312
2302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d
6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a
92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4d
d9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87d
d3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e04160414
d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009
060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307130d4d6f756e7461696e20566965577311030300e060355040a1307416e6
4726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e6
4726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010019d30cf105fb78923f4c0d7dd223233
d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e6181
86673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c196
2fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb
21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b

SxHy+zpC+eGmQUPW4BYYcldQdVxiSSVnY0gIrWauGKU=

☰ SCAN LOGS

Timestamp	Event	Error
2025-08-29 20:10:42	Generating Hashes	OK
2025-08-29 20:10:42	Extracting APK	OK
2025-08-29 20:10:42	Unzipping	OK
2025-08-29 20:10:42	Parsing APK with androguard	OK
2025-08-29 20:10:45	Extracting APK features using aapt/aapt2	OK
2025-08-29 20:10:46	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 20:10:50	Parsing AndroidManifest.xml	OK
2025-08-29 20:10:50	Extracting Manifest Data	OK
2025-08-29 20:10:50	Manifest Analysis Started	OK
2025-08-29 20:10:50	Performing Static Analysis on: Blood Sugar (com.blood.sugar.diabetes.tracker)	OK

2025-08-29 20:10:50	Fetching Details from Play Store: com.blood.sugar.diabetes.tracker	OK
2025-08-29 20:10:51	Checking for Malware Permissions	OK
2025-08-29 20:10:51	Fetching icon path	OK
2025-08-29 20:10:51	Library Binary Analysis Started	OK
2025-08-29 20:10:51	Reading Code Signing Certificate	OK
2025-08-29 20:10:52	Running APKiD 2.1.5	OK
2025-08-29 20:10:56	Detecting Trackers	OK
2025-08-29 20:10:58	Decompiling APK to Java with JADX	OK
2025-08-29 20:11:17	Converting DEX to Smali	OK
2025-08-29 20:11:17	Code Analysis Started on - java_source	OK

2025-08-29 20:11:21	Android SBOM Analysis Completed	OK
2025-08-29 20:11:32	Android SAST Completed	OK
2025-08-29 20:11:32	Android API Analysis Started	OK
2025-08-29 20:11:43	Android API Analysis Completed	OK
2025-08-29 20:11:44	Android Permission Mapping Started	OK
2025-08-29 20:11:53	Android Permission Mapping Completed	OK
2025-08-29 20:11:53	Android Behaviour Analysis Started	OK
2025-08-29 20:12:07	Android Behaviour Analysis Completed	OK
2025-08-29 20:12:07	Extracting Emails and URLs from Source Code	OK
2025-08-29 20:12:13	Email and URL Extraction Completed	OK
2025-08-29 20:12:13	Extracting String data from APK	OK

2025-08-29 20:12:16	Extracting String data from Code	OK
2025-08-29 20:12:16	Extracting String values and entropies from Code	OK
2025-08-29 20:12:19	Performing Malware check on extracted domains	OK
2025-08-29 20:12:54	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.