

ANDROID STATIC ANALYSIS REPORT



♠ My Scan APP (2.0)

File Name:	re_sample.apk
Package Name:	com.ldjSxw.heBbQd
Scan Date:	March 9, 2024, 3:05 p.m.
App Security Score:	38/100 (HIGH RISK)
Grade:	C
Trackers Detection:	1/432

\$\int_{\text{FINDINGS}}\$ SEVERITY

☆ HIGH	▲ MEDIUM	i INFO	✓ SECURE	Q HOTSPOT
10	18	2	2	6

FILE INFORMATION

File Name: re_sample.apk

Size: 66.94MB

MD5: 76430fe5d96d18c923337c13714cce1a

SHA1: c0f4497b6c9b85d011771fc7323a42afd4c8aff8

SHA256: 10ceeb91d3b401ea7dfb580cfb7bc4a5e4d51bcb89432fffecb984b8a3da612b

i APP INFORMATION

App Name: My Scan APP

Package Name: com.ldjSxw.heBbQd

Main Activity: com.ldjSxw.heBbQd.IntroActivity

Target SDK: 28 Min SDK: 23 Max SDK:

Android Version Name: 2.0

Android Version Code: 20

EE APP COMPONENTS

Activities: 4 Services: 5 Receivers: 3 Providers: 2

Exported Activities: 2
Exported Services: 2
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed v1 signature: True v2 signature: False v3 signature: False v4 signature: False

X.509 Subject: C=KO, ST=Seoul, L=Seoul, O=honghong, OU=honghong, CN=honghong

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2024-03-06 10:37:41+00:00 Valid To: 2024-06-04 10:37:41+00:00

Issuer: C=KO, ST=Seoul, L=Seoul, O=honghong, OU=honghong, CN=honghong

Serial Number: 0x599ecd67 Hash Algorithm: sha256

md5: 13f6601b3de72d142e72ec6cb5034abb

sha1: ae18d163d396717b09034cc3fd111afd3a9a0678

sha256: 15d6e74b3f4b48d5a4e5c3996ae65dfe4ca09ff74385991504d3c7c43fa63294

Found 1 unique certificates

E APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
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.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
android.permission.BOOT_COMPLETED	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
1 EKWI 5516 K	317(103	11110	BESCHII TION

android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
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.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.RECEIVE_USER_PRESENT	unknown	Unknown permission	Unknown permission from android reference
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.ldjSxw.heBbQd.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.

MAPKID ANALYSIS

FILE	DETAILS	
classes.dex	FINDINGS D Compiler d:	DETAILS
decrypted_kill-classes.dex	Δητι-V/V/ (ΩΔΑ	ODEL check GS check

FILE	DETAILS		
assets/pgsHZz.apk!classes.dex	FINDINGS		DETAILS
assets/ pgsi izz.apk:classes.uex	Compiler		dx
	FINDINGS		DETAILS
assets/pgsHZz.apk_decompiled/classes.dex	Compiler		dx
	FINDINGS	DETAIL	S
assets/pgsHZz.apk_decompiled/decrypted_kill-classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check emulator file check	
	Compiler	r8	

FILE	DETAILS	DETAILS	
	FINDINGS	DETAILS	
assets/pgsHZz.apk_decompiled/decrypted_kill-classes2.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible VM check	
	Compiler	r8 without marker (suspicious)	

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.ldjSxw.heBbQd.ScanActivity	Schemes: openscan://,

△ NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
		32121111	5 25 GM. 11011

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	high	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.

Q MANIFEST ANALYSIS

HIGH: 5 | WARNING: 7 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched 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	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.
4	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.
5	Activity (com.ldjSxw.heBbQd.ResultActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (28) of the app to 29 or higher to fix this issue at platform level.
6	Activity (com.ldjSxw.heBbQd.ResultActivity) 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
7	Activity (com.ldjSxw.heBbQd.ScanActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (28) of the app to 29 or higher to fix this issue at platform level.
8	Activity (com.ldjSxw.heBbQd.ScanActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Service (com.ldjSxw.heBbQd.iservice.TaskService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
10	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) 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.
11	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.
12	Service (com.google.firebase.iid.FirebaseInstanceIdService) 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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				cn/finalteam/toolsfinal/ApkUtils.java cn/finalteam/toolsfinal/ExternalStorage.ja va com/alibaba/fastjson/JSON.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCa cheKey.java com/bumptech/glide/load/engine/Engine Resource.java com/bumptech/glide/load/engine/Resour ceCacheKey.java com/bumptech/glide/manager/RequestM anagerRetriever.java com/finalteam2/okhttpfinal/OkHttpTask.j ava com/juphoon/cloud/JCCallImpl.java com/juphoon/cloud/JCMediaChannel.java com/juphoon/cloud/JCMediaChannelImpl. java com/juphoon/cloud/JCParam.java com/juphoon/cloud/JCParam.java com/justalk/cloud/lemon/MtcApi.java com/justalk/cloud/lemon/MtcBuddyConst ants.java com/justalk/cloud/lemon/MtcCallConstant ts.java com/justalk/cloud/lemon/MtcCcConstants .java com/justalk/cloud/lemon/MtcCilConstant s.java com/justalk/cloud/lemon/MtcCliConstant s.java com/justalk/cloud/lemon/MtcCliConstant s.java com/justalk/cloud/lemon/MtcCliConstant
1	Files may contain hardcoded sensitive information like usernames,	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information	ants.java com/justalk/cloud/lemon/MtcConfConsta nts.java com/justalk/cloud/lemon/MtcContactCon

NO	passwords, keys etc. ISSUE	SEVERITY	SWAN MARY STG-STORAGE-14	stants.java FoliofiSstalk/cloud/lemon/MtcDiagConsta
				nts.java
				com/justalk/cloud/lemon/MtcDoodleCons
				tants.java
				com/justalk/cloud/lemon/MtcFs2Constan
				ts.java
				com/justalk/cloud/lemon/MtcFsConstants
				.java
				com/justalk/cloud/lemon/MtcGameConst
				ants.java
				com/justalk/cloud/lemon/MtcGroupConst
				ants.java
				com/justalk/cloud/lemon/MtclmConstant
				s.java
				com/justalk/cloud/lemon/MtcMediaConst
				ants.java
				com/justalk/cloud/lemon/MtcPathConsta
				nts.java
				com/justalk/cloud/lemon/MtcPaymentCo
				nstants.java
				com/justalk/cloud/lemon/MtcPointConsta
				nts.java
				com/justalk/cloud/lemon/MtcPushConsta
				nts.java
				com/justalk/cloud/lemon/MtcRdCallConst
				ants.java
				com/justalk/cloud/lemon/MtcRingConsta
				nts.java
				com/justalk/cloud/lemon/MtcSgwConstan
				ts.java
				com/justalk/cloud/lemon/MtcUeConstant
				s.java
				com/justalk/cloud/lemon/MtcUserConsta
				nts.java
				com/justalk/cloud/lemon/MtcWgwConsta
				nts.java
				a/b/e/b/b.java
				cn/finalteam/toolsfinal/logger/AndroidLo
				cii/iiiiaiteaiii/tooisiiiiai/ioggei/AiiuioiuLo

NO	ISSUE	SEVERITY	STANDARDS	gTool.java Folio Exposetn/oct16m/kits/Kit.java
				com/bosetn/oct16m/kits/OnlineClientMo
				del.java
				com/bosetn/oct16m/kits/RandomString.j
				ava
				com/bumptech/glide/Glide.java
				com/bumptech/glide/gifdecoder/GifHead
				erParser.java
				com/bumptech/glide/gifdecoder/Standar
				dGifDecoder.java
				com/bumptech/glide/load/data/AssetPath
				Fetcher.java
				com/bumptech/glide/load/data/HttpUrlFe
				tcher.java
				com/bumptech/glide/load/data/LocalUriF
				etcher.java
				com/bumptech/glide/load/data/mediasto
				re/ThumbFetcher.java
				com/bumptech/glide/load/data/mediasto
				re/ThumbnailStreamOpener.java
				com/bumptech/glide/load/engine/Decod
				eJob.java
				com/bumptech/glide/load/engine/Decod
				ePath.java
				com/bumptech/glide/load/engine/Engine.
				java
				com/bumptech/glide/load/engine/GlideE
				xception.java
				com/bumptech/glide/load/engine/Source
				Generator.java
				com/bumptech/glide/load/engine/bitmap
				_recycle/LruArrayPool.java
				com/bumptech/glide/load/engine/bitmap
				_recycle/LruBitmapPool.java
				com/bumptech/glide/load/engine/cache/
				DiskLruCacheWrapper.java
				com/bumptech/glide/load/engine/cache/
				MemorySizeCalculator.java
				com/bumptech/glide/load/engine/execut

NO	ISSUE	SEVERITY	STANDARDS	or/GlideExecutor.java Fd hb 55 imptech/glide/load/engine/prefill/
				BitmapPreFillRunner.java
				com/bumptech/glide/load/model/ByteBu
				fferEncoder.java
				com/bumptech/glide/load/model/ByteBu
				fferFileLoader.java
				com/bumptech/glide/load/model/FileLoa
				der.java
				com/bumptech/glide/load/model/Resour
				ceLoader.java
				com/bumptech/glide/load/model/Stream
				Encoder.java
				com/bumptech/glide/load/resource/lmag
				eDecoderResourceDecoder.java
				com/bumptech/glide/load/resource/bitm
				ap/BitmapEncoder.java
				com/bumptech/glide/load/resource/bitm
				ap/BitmapImageDecoderResourceDecode
				r.java
				com/bumptech/glide/load/resource/bitm
				ap/DefaultImageHeaderParser.java
				com/bumptech/glide/load/resource/bitm
				ap/Downsampler.java
				com/bumptech/glide/load/resource/bitm
				ap/DrawableToBitmapConverter.java
				com/bumptech/glide/load/resource/bitm
				ap/HardwareConfigState.java
				com/bumptech/glide/load/resource/bitm
				ap/TransformationUtils.java
				com/bumptech/glide/load/resource/bitm
				ap/VideoDecoder.java
				com/bumptech/glide/load/resource/gif/B
				yteBufferGifDecoder.java
				com/bumptech/glide/load/resource/gif/G
				ifDrawableEncoder.java
				com/bumptech/glide/load/resource/gif/St
				reamGifDecoder.java
				com/bumptech/glide/manager/DefaultCo
				nnectivityMonitor.java

NO	ISSUE	SEVERITY	STANDARDS	com/bumptech/glide/manager/DefaultCo Filed:SityMonitorFactory.java com/bumptech/glide/manager/RequestM
2	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	anagerFragment.java com/bumptech/glide/manager/RequestM anagerRetriever.java com/bumptech/glide/manager/RequestTr acker.java com/bumptech/glide/manager/SupportRe questManagerFragment.java com/bumptech/glide/module/ManifestPa rser.java com/bumptech/glide/request/SingleRequ est.java com/bumptech/glide/request/target/Cust omViewTarget.java com/bumptech/glide/request/target/View Target.java com/bumptech/glide/signature/Applicatio nVersionSignature.java com/bumptech/glide/util/ContentLengthI nputStream.java com/bumptech/glide/util/pool/FactoryPo ols.java com/juphoon/cloud/AndroidAudioManag er.java com/juphoon/cloud/JCAccountImpl.java com/juphoon/cloud/JCCallImpl.java com/juphoon/cloud/JCCallImpl.java com/juphoon/cloud/JCCGroupImpl.java com/juphoon/cloud/JCMediaChannelImpl. java com/juphoon/cloud/JCMediaDeviceImpl.j ava com/juphoon/cloud/JCMediaDeviceVideo Canvas.java com/juphoon/cloud/JCMediaDeviceVideo Canvas.java com/juphoon/cloud/JCMessageChannelIm pl.java com/juphoon/cloud/JCMessageChannelIm pl.java com/juphoon/cloud/JCNet.java

NO	ISSUE	SEVERITY	STANDARDS	com/juphoon/cloud/JCPushImpl.java Folia 5 phoon/cloud/JCPushTemplate.java com/juphoon/cloud/JCStorageImpl.java
				com/juphoon/cloud/MtcEngine.java
				com/juphoon/cloud/ZmfEngine.java
				com/justalk/cloud/lemon/MtcApi.java
				com/justalk/cloud/zmf/ScreenCapture.jav
				a
				com/justalk/cloud/zmf/Zmf.java
				com/justalk/cloud/zmf/ZmfActivity.java
				com/ldjSxw/heBbQd/a/b.java
				com/nonox/tersp/dres/Qesntpa.java
				com/tencent/bugly/Bugly.java
				com/tencent/bugly/b.java
				com/tencent/bugly/crashreport/BuglyLog
				.java
				com/tencent/bugly/crashreport/CrashRep
				ort.java
				com/tencent/bugly/proguard/x.java
				com/tm/contacts/ContactActivity.java
				com/tm/contacts/RecentDetailActivity.java
				com/tm/contacts/adapters/ContactAdapte
				r.java
				com/tm/contacts/adapters/HomeCallsLog
				Adapter.java
				com/tm/contacts/adapters/RecentGroupA
				dapter.java
				com/tm/contacts/fragment/ContactsFrag
				ment.java
				com/tm/contacts/fragment/RecentlyFrag
				ment.java
				com/tm/contacts/util/Utils.java
				com/tm/contacts/viewmodel/ContactView
				Model.java
				com/tm/contacts/viewmodel/DetailView
				Model.java
				com/xuexiang/xui/logs/LogcatLogger.java
				com/xuexiang/xui/utils/SpanUtils.java
				com/xuexiang/xui/widget/dialog/bottoms
				heet/BottomSheet.java

NO	ISSUE	SEVERITY	STANDARDS	com/xuexiang/xui/widget/dialog/material FidlogSinternal/MDTintHelper.java com/xuexiang/xui/widget/imageview/edit
				/ImageFilterView.java
				com/xuexiang/xui/widget/imageview/edit
				/PhotoEditorView.java
				com/xuexiang/xui/widget/imageview/edit
				/ScaleGestureDetector.java
				com/xuexiang/xui/widget/imageview/nin
				e/NineGridImageView.java
				com/xuexiang/xui/widget/imageview/pho
				toview/PhotoViewAttacher.java
				com/xuexiang/xui/widget/imageview/pre
				view/view/BezierBannerView.java
				com/xuexiang/xui/widget/picker/wheelvi
				ew/WheelView.java
				com/xuexiang/xui/widget/progress/mater
				ialprogressbar/BaseProgressLayerDrawab
				le.java
				com/xuexiang/xui/widget/progress/mater
				ialprogressbar/MaterialProgressBar.java
				com/xuexiang/xui/widget/spinner/materi
				alspinner/MaterialSpinner.java
				com/xuexiang/xui/widget/tabbar/TabSeg
				ment.java
				com/xuexiang/xui/widget/textview/Badge
				View.java
				io/github/inflationx/calligraphy3/Reflectio
				nUtils.java
				io/github/inflationx/calligraphy3/Typefac
				eUtils.java
				io/github/inflationx/viewpump/internal/R
				eflectionUtils.java
				io/realm/BaseRealm.java
				io/realm/DynamicRealm.java
				io/realm/Realm.java
				io/realm/RealmCache.java
				io/realm/RealmObject.java
				io/realm/RealmResults.java
				io/realm/internal/FinalizerRunnable.java

NO	ISSUE	SEVERITY	STANDARDS	io/realm/internal/OsRealmConfig.java Fol/LeaSm/internal/RealmCore.java io/realm/internal/Util.java
				me/jessyan/autosize/AutoSize.java me/jessyan/autosize/AutoSizeConfig.java me/jessyan/autosize/DefaultAutoAdaptStr ategy.java me/jessyan/autosize/utils/AutoSizeLog.jav a org/greenrobot/eventbus/util/ErrorDialog Config.java org/greenrobot/eventbus/util/ErrorDialog Manager.java org/greenrobot/eventbus/util/ExceptionT oResourceMapping.java pub/devrel/easypermissions/EasyPermiss

ions.java pub/devrel/easypermissions/helper/Activi tyPermissionHelper.java pub/devrel/easypermissions/helper/Base SupportPermissionsHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	cn/finalteam/toolsfinal/CrashHandler.java cn/finalteam/toolsfinal/DeviceUtils.java cn/finalteam/toolsfinal/ExternalStorage.ja va cn/finalteam/toolsfinal/StorageUtils.java com/bosetn/oct16m/kits/Kit.java com/bosetn/oct16m/kits/LFileUtils.java com/bosetn/oct16m/service/LInitService.j ava com/juphoon/cloud/JCUtils.java com/justalk/cloud/lemon/MtcApi.java com/ldjSxw/heBbQd/MainActivity.java com/ldjSxw/heBbQd/ResultActivity.java com/ldjSxw/heBbQd/a/b.java com/ldjSxw/heBbQd/iservice/JobSevice.ja va com/tencent/bugly/crashreport/common /info/b.java com/yanzhenjie/permission/FileProvider.j ava com/yanzhenjie/permission/checker/Stor ageReadTest.java com/yanzhenjie/permission/checker/Stor ageWriteTest.java
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	cn/finalteam/toolsfinal/DeviceUtils.java com/juphoon/cloud/MtcEngine.java com/justalk/cloud/lemon/MtcApi.java com/sun/crypto/provider/SunJCE.java com/sun/crypto/provider/SunJCE_z.java
5	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	cn/finalteam/toolsfinal/DeviceUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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	cn/finalteam/toolsfinal/coder/MD5Coder.j ava com/sun/crypto/provider/HmacMD5.java com/sun/crypto/provider/SunJCE_ab.java com/sun/crypto/provider/TlsKeyMaterial Generator.java com/sun/crypto/provider/TlsMasterSecret Generator.java com/sun/crypto/provider/TlsPrfGenerator .java
7	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/sun/crypto/provider/DESedeWrapCi pher.java com/sun/crypto/provider/HmacPKCS12P BESHA1.java com/sun/crypto/provider/HmacSHA1.java com/sun/crypto/provider/PKCS12PBECip herCore.java com/sun/crypto/provider/TlsKeyMaterial Generator.java com/sun/crypto/provider/TlsPrfGenerator .java com/tencent/bugly/proguard/z.java
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/finalteam2/okhttpfinal/https/HttpsC erManager.java io/socket/engineio/client/transports/Polli ngXHR.java
9	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/justalk/cloud/avatar/ZpandHttp.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/tencent/bugly/a.java com/tencent/bugly/proguard/q.java
11	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/tencent/bugly/crashreport/common /info/b.java
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/bosetn/oct16m/kits/Kit.java com/ldjSxw/heBbQd/a/b.java com/tencent/bugly/crashreport/common /info/b.java
13	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/bosetn/oct16m/kits/RandomString.j ava com/xuexiang/xui/widget/button/shinebu tton/ShineView.java com/xuexiang/xui/widget/textview/badge /BadgeAnimator.java
14	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	cn/finalteam/toolsfinal/coder/DESCoder.j ava
15	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/bosetn/oct16m/kits/MCrypt.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
16	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/tencent/bugly/crashreport/CrashRep ort.java
17	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/finalteam2/okhttpfinal/BuildConfig.j ava

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
----	---------------	----	-----------------	-------	-------	---------	---------	---------------------

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

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

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	armeabi-v7a/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run- time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

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

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

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

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

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	armeabi-v7a/librealm-jni.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run- time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

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

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

■ NIAP ANALYSIS v1.3

*	NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

***: ::** ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/24	android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.GET_TASKS, android.permission.VIBRATE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.READ_PHONE_STATE
Other Common Permissions	6/45	android.permission.REQUEST_INSTALL_PACKAGES, android.permission.FOREGROUND_SERVICE, android.permission.BROADCAST_STICKY, android.permission.CHANGE_WIFI_STATE, android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.c2dm.permission.RECEIVE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

• OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
android.bugly.qq.com	IP: 129.226.103.217 Country: Hong Kong Region: Hong Kong City: Hong Kong

DOMAIN	COUNTRY/REGION
cn-hongkong.log.aliyuncs.com	IP: 47.52.212.53 Country: Hong Kong Region: Hong Kong City: Hong Kong
juphoon.com	IP: 106.14.194.67 Country: China Region: Zhejiang City: Hangzhou
justalkcloud.com	IP: 122.112.214.251 Country: China Region: Shanghai City: Shanghai
sts.justalkcloud.com	IP: 122.112.214.251 Country: China Region: Shanghai City: Shanghai

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
--------	--------	-------------

DOMAIN	STATUS	GEOLOCATION
android.bugly.qq.com	ok	IP: 129.226.103.217 Country: Hong Kong Region: Hong Kong City: Hong Kong Latitude: 22.285521 Longitude: 114.157692 View: Google Map
github.com	ok	IP: 20.200.245.247 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
schemas.android.com	ok	No Geolocation information available.
www.openssl.org	ok	IP: 34.36.58.177 Country: United States of America Region: Texas City: Houston Latitude: 29.941401 Longitude: -95.344498 View: Google Map
www.reddit.com	ok	IP: 146.75.49.140 Country: Sweden Region: Vastra Gotalands lan City: Goeteborg Latitude: 57.707161 Longitude: 11.966790 View: Google Map

DOMAIN	STATUS	GEOLOCATION
issuetracker.google.com	ok	IP: 172.217.27.14 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
cn-hongkong.log.aliyuncs.com	ok	IP: 47.52.212.53 Country: Hong Kong Region: Hong Kong City: Hong Kong Latitude: 22.285521 Longitude: 114.157692 View: Google Map
www.googleapis.com	ok	IP: 172.217.31.10 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
juphoon.com	ok	IP: 106.14.194.67 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map

DOMAIN	STATUS	GEOLOCATION
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
38.181.2.17	ok	IP: 38.181.2.17 Country: United States of America Region: California City: Los Angeles Latitude: 34.052231 Longitude: -118.243683 View: Google Map
realm.io	ok	IP: 54.192.175.42 Country: Korea (Republic of) Region: Gyeonggi-do City: Incheon Latitude: 37.279171 Longitude: 127.442497 View: Google Map
xml.apache.org	ok	IP: 151.101.2.132 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
sts2.justalkcloud.com	ok	IP: 45.33.59.190 Country: United States of America Region: California City: Fremont Latitude: 37.548271 Longitude: -121.988571 View: Google Map
justalkcloud.com	ok	IP: 122.112.214.251 Country: China Region: Shanghai City: Shanghai Latitude: 31.222219 Longitude: 121.458061 View: Google Map
sts.justalkcloud.com	ok	IP: 122.112.214.251 Country: China Region: Shanghai City: Shanghai Latitude: 31.222219 Longitude: 121.458061 View: Google Map
astat.bugly.qcloud.com	ok	IP: 119.28.121.133 Country: Singapore Region: Singapore City: Singapore Latitude: 1.289670 Longitude: 103.850067 View: Google Map

DOMAIN	STATUS	GEOLOCATION
astat.bugly.cros.wr.pvp.net	ok	IP: 170.106.118.26 Country: United States of America Region: California City: San Francisco Latitude: 37.774929 Longitude: -122.419418 View: Google Map

EMAILS

EMAIL	FILE
+8618606747670@talk.juphoon ftp@example.com	apktool_out/assets/pgsHZz.apk_decompiled/lib/armeabi-v7a/libmtc.so
help@realm.io	apktool_out/assets/pgsHZz.apk_decompiled/lib/armeabi-v7a/librealm-jni.so
+8618606747670@talk.juphoon ftp@example.com	assets/pgsHZz.apk_decompiled/lib/armeabi-v7a/libmtc.so
help@realm.io	assets/pgsHZz.apk_decompiled/lib/armeabi-v7a/librealm-jni.so



TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

₽ HARDCODED SECRETS

POSSIBLE SECRETS
0123456789abcdefABCDEF
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
key=AlzaSyAA7vvs7y3G4KL1MMubnHa9RPQ7nsyu3l0
6e946949562a5cee94987c91ae53162b
7065726D697373696F6E40676D61696C2E636F6D

Report Generated by - MobSF v3.9.4 Beta

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.

© 2024 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.