

ANDROID STATIC ANALYSIS REPORT



sonqLgOT (3.0.2)

File Name: re_pgsHZz.apk

Package Name: com.bosetn.oct16m

Scan Date: March 9, 2024, 10:13 a.m.

App Security Score:

43/100 (MEDIUM RISK)

Grade:

В

Trackers Detection:

2/432

\$ FINDINGS SEVERITY

兼 HIGH	▲ MEDIUM	i INFO	✓ SECURE	% НОТЅРОТ
8	33	2	2	6



File Name: re_pgsHZz.apk

Size: 32.17MB

MD5: 8f7ec82f3753fb65a94a8befd8e535f0

SHA1: fc4211da5d615e5743f6f0158a930c53d45443ff

SHA256: 301c13401f3552dbeb01935ff8cf768b912c92f6b42d0daeb951827316f97391

i APP INFORMATION

App Name: sonqLgOT

Package Name: com.bosetn.oct16m

Main Activity: Target SDK: 26 Min SDK: 21 Max SDK:

Android Version Name: 3.0.2
Android Version Code: 302

APP COMPONENTS

Activities: 16 Services: 12 Receivers: 8 Providers: 5 Exported Activities

Exported Activities: 6 Exported Services: 5 Exported Receivers: 7 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=jobjo, L=jobjo, O=jobjo, OU=jobjo, CN=jobjo

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2024-03-07 03:00:46+00:00 Valid To: 2024-06-05 03:00:46+00:00

Issuer: C=ko, ST=jobjo, L=jobjo, O=jobjo, OU=jobjo, CN=jobjo

Serial Number: 0x4d31f258 Hash Algorithm: sha256

md5: 4db46c1b5ea2f846f62efeb523406793 sha1: b4f978c27cc22122df6fcbbe9a84fd8ae063b03f

sha256: 28a9680feedbbf5d0936e71c0ae56abf0865359bb02a5756f29017d2d9aaf15d

sha512: 788d20553b25a5045c52e6 fea4e30d4e92322454ad3a9c3fc5ad02bd403aef055b7cc6e49def1b2c673e5e09509ec60614ed987d0c9f8d0942259d676016c1f5

Found 1 unique certificates

E APPLICATION PERMISSIONS

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.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
android.permission.READ_CALL_LOG	dangerous	grants read access to the user's call log.	Allows an application to read the user's call log.
android.permission.WRITE_CALL_LOG	dangerous	allows writing to (but not reading) the user's call log.	Allows an application to write (but not read) the user's call log data.
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.
android.permission.ACCESS_NETWORK_STATE normal view network status		view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK normal prev		prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.GET_TASKS da		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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BROADCAST_STICKY	ssion.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.PROCESS_OUTGOING_CALLS	dangerous	intercept outgoing calls	Allows application to process outgoing calls and change the number to be dialled. Malicious applications may monitor, redirect or prevent outgoing calls.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.RECEIVE_SMS dangerous receive SMS		Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.	
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
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.
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
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.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.ACTION_MANAGE_OVERLAY_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.READ_PHONE_NUMBERS	dangerous	allows reading of the device's phone number(s).	Allows read access to the device's phone number(s). This is a subset of the capabilities granted by READ_PHONE_STATE but is exposed to instant applications.
android.permission.RECEIVE_MMS	dangerous	receive MMS	Allows application to receive and process MMS messages. Malicious applications may monitor your messages or delete them without showing them to you.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BOOT_COMPLETED	unknown	Unknown permission	Unknown permission from android reference
com.bosetn.oct16m.andpermission.bridge	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.bosetn.oct16m.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	dangerous	mount and unmount file systems	Allows the application to mount and unmount file systems for removable storage.

APKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS		DETAILS
Classes.uex	Compiler		dx
	FINDINGS	DETAILS	
decrypted_kill-classes.dex	Anti-VM Code	Build.FINGERPRINT of Build.MODEL check Build.MANUFACTUR Build.PRODUCT check Build.HARDWARE ch Build.BOARD check possible Build.SERIA Build.TAGS check SIM operator check emulator file check	ER check ck eck
	Compiler	r8	

FILE	DETAILS		
	FINDINGS	DETAILS	
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.bosetn.oct16m.CallActivity	Schemes: tel://,
com.bosetn.oct16m.ActionActivity	Schemes: omgodomja://,
com.bosetn.oct16m.ComPoseActivity	Schemes: sms://, smsto://, mms://, mmsto://,

△ NETWORK SECURITY

NO SCOPE SEVERITY DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

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

TITLE	SEVERITY	DESCRIPTION
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: 3 | WARNING: 22 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	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.
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.bosetn.oct16m.MainActivity) 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.
6	Activity (com.bosetn.oct16m.PermissionActivity) 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.
7	Activity (com.bosetn.oct16m.CallActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
8	Activity (com.bosetn.oct16m.ActionActivity) 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
9	Service (com.bosetn.oct16m.service.LCallService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_INCALL_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
10	Service (com.bosetn.oct16m.service.LAutoService) 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.
11	Broadcast Receiver (com.bosetn.oct16m.receiver.LOutReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
12	Broadcast Receiver (com.bosetn.oct16m.receiver.LPReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
13	Broadcast Receiver (com.bosetn.oct16m.receiver.LBootReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
14	Broadcast Receiver (com.bosetn.oct16m.receiver.LSMReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BROADCAST_SMS [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.
15	Broadcast Receiver (com.bosetn.oct16m.receiver.LMSReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BROADCAST_WAP_PUSH [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.
16	Activity (com.bosetn.oct16m.ComPoseActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
17	Service (com.bosetn.oct16m.service.MIDService) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Service is explicitly exported.
18	Activity (com.tm.contacts.ContactActivity) 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.
19	Service (com.google.firebase.messaging.FirebaseMessagingService) 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.
20	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.
21	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.
22	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.
23	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
24	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
25	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	cn/finalteam/toolsfinal/ApkUtils.java cn/finalteam/toolsfinal/ExternalStorage.java com/alibaba/fastjson/JSON.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.j ava com/juphoon/cloud/JCGIllmpl.java com/juphoon/cloud/JCGGrouplmpl.java com/juphoon/cloud/JCMediaChannel.java com/juphoon/cloud/JCMediaChannelImpl.java com/juphoon/cloud/JCMediaChannelImpl.java com/juphoon/cloud/JCMediaChannelImpl.java com/juphoon/cloud/JCParam.java com/justalk/cloud/JCParam.java com/justalk/cloud/lemon/MtcApi.java com/justalk/cloud/lemon/MtcBuddyConstants.java com/justalk/cloud/lemon/MtcCollConstants.java com/justalk/cloud/lemon/MtcCollConstants.java com/justalk/cloud/lemon/MtcConf2Constants.java com/justalk/cloud/lemon/MtcConf2Constants.java com/justalk/cloud/lemon/MtcConfConstants.java com/justalk/cloud/lemon/MtcDodleConstants.java com/justalk/cloud/lemon/MtcPs2Constants.java com/justalk/cloud/lemon/MtcFs2Constants.java com/justalk/cloud/lemon/MtcGameConstants.java com/justalk/cloud/lemon/MtcGameConstants.java com/justalk/cloud/lemon/MtcGameConstants.java com/justalk/cloud/lemon/MtcGameConstants.java com/justalk/cloud/lemon/MtcGameConstants.java com/justalk/cloud/lemon/MtcPathConstants.java com/justalk/cloud/lemon/MtcPontConstants.java com/justalk/cloud/lemon/MtcPontConstants.java com/justalk/cloud/lemon/MtcRopamentConstants.java com/justalk/cloud/lemon/MtcPontConstants.java com/justalk/cloud/lemon/MtcPontConstants.java com/justalk/cloud/lemon/MtcPontConstants.java com/justalk/cloud/lemon/MtcPontConstants.java com/justalk/cloud/lemon/MtcPontConstants.java com/justalk/cloud/lemon/MtcPontConstants.java com/justalk/cloud/lemon/MtcPontConstants.java com/justalk/cloud/lemon/MtcPontConstants.java com/justalk/cloud/lemon/MtcPontConstants.java com/justalk/cloud/lemon/MtcUserConstants.java com/just
				cn/finalteam/toolsfinal/logger/AndroidLogTool.java com/bosetn/oct16m/kits/Kit.java com/bosetn/oct16m/kits/OnlineClientModel.java com/bosetn/oct16m/kits/RandomString.java com/bumptech/glide/Glide.java

NO	ISSUE	SEVERITY	STANDARDS	com/bumptech/glide/gifdecoder/GifHeaderParser.java Fd lan
	13332		31/112/1123	com/bumptech/glide/load/data/AssetPathFetcher.java
				com/bumptech/glide/load/data/HttpUrlFetcher.java
				com/bumptech/glide/load/data/LocalUriFetcher.java
				com/bumptech/glide/load/data/mediastore/ThumbFetche
				r.java
				com/bumptech/glide/load/data/mediastore/ThumbnailStr
				eamOpener.java
				com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java
				com/bumptech/glide/load/engine/Engine.java
				com/bumptech/glide/load/engine/GlideException.java
				com/bumptech/glide/load/engine/SourceGenerator.java
				com/bumptech/glide/load/engine/bitmap_recycle/LruArra
				yPool.java
				com/bumptech/glide/load/engine/bitmap_recycle/LruBit
				mapPool.java
				com/bumptech/glide/load/engine/cache/DiskLruCacheWr
				apper.java
				com/bumptech/glide/load/engine/cache/MemorySizeCalc ulator.java
				com/bumptech/glide/load/engine/executor/GlideExecutor
				.java
				com/bumptech/glide/load/engine/prefill/BitmapPreFillRu
				nner.java
				com/bumptech/glide/load/model/ByteBufferEncoder.java
				com/bumptech/glide/load/model/ByteBufferFileLoader.ja
				va
				com/bumptech/glide/load/model/FileLoader.java
				com/bumptech/glide/load/model/ResourceLoader.java
				com/bumptech/glide/load/model/StreamEncoder.java
				com/bumptech/glide/load/resource/ImageDecoderResour
				ceDecoder.java
				com/bumptech/glide/load/resource/bitmap/BitmapEncod
				er.java
				com/bumptech/glide/load/resource/bitmap/BitmapImage
				DecoderResourceDecoder.java
				com/bumptech/glide/load/resource/bitmap/DefaultImage HeaderParser.java
				com/bumptech/glide/load/resource/bitmap/Downsample
				r.java
				com/bumptech/glide/load/resource/bitmap/DrawableToB
				itmapConverter.java
				com/bumptech/glide/load/resource/bitmap/HardwareCo
				nfigState.java
				com/bumptech/glide/load/resource/bitmap/Transformati
				onUtils.java
				com/bumptech/glide/load/resource/bitmap/VideoDecode
				r.java
				com/bumptech/glide/load/resource/gif/ByteBufferGifDec
				oder.java

NO	ISSUE	SEVERITY	STANDARDS	com/bumptech/glide/load/resource/gif/GifDrawableEnco
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	com/bumptech/glide/Inad/resource/gif/StreamGifDecode r.java com/bumptech/glide/manager/DefaultConnectivityMonito r.java com/bumptech/glide/manager/DefaultConnectivityMonito rFactory.java com/bumptech/glide/manager/RequestManagerFragment .java com/bumptech/glide/manager/RequestManagerRetriever.j ava com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SupportRequestManagerFr agment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.ja va com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignatu re.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/ContentLengthInputStream.java com/juphoon/cloud/JCAccountImpl.java com/juphoon/cloud/JCCallImpl.java com/juphoon/cloud/JCCallImpl.java com/juphoon/cloud/JCGcountImpl.java com/juphoon/cloud/JCGoodleImpl.java com/juphoon/cloud/JCGroupImpl.java com/juphoon/cloud/JCMediaDeviceImpl.java com/juphoon/cloud/JCMediaDeviceImpl.java com/juphoon/cloud/JCMediaDeviceVideoCanvas.java com/juphoon/cloud/JCMediaDeviceVideoCanvas.java com/juphoon/cloud/JCNediaDeviceImpl.java com/juphoon/cloud/JCNediaDeviceImpl.java com/juphoon/cloud/JCNediaDeviceImpl.java com/juphoon/cloud/JCNessageChannelImpl.java

NO	ISSUE	SEVERITY	STANDARDS	com/tm/contacts/adapters/ContactAdapter.java ស្រី៤៤វិសា/contacts/adapters/HomeCallsLogAdapter.java
				com/tm/contacts/fragment/ContactsFragment.java com/tm/contacts/fragment/RecentlyFragment.java com/tm/contacts/viel/Utils.java com/tm/contacts/viewmodel/ContactViewModel.java com/tm/contacts/viewmodel/DetailViewModel.java com/tm/contacts/viewmodel/DetailViewModel.java com/tm/contacts/viewmodel/DetailViewModel.java com/xuexiang/xui/logs/LogcatLogger.java com/xuexiang/xui/widget/dialog/bottomsheet/BottomShe et.java com/xuexiang/xui/widget/dialog/materialdialog/internal/ MDTintHelper.java com/xuexiang/xui/widget/imageview/edit/ImageFilterVie w.java com/xuexiang/xui/widget/imageview/edit/PhotoEditorVie w.java com/xuexiang/xui/widget/imageview/edit/ScaleGestureDe tector.java com/xuexiang/xui/widget/imageview/nine/NineGridImage View.java com/xuexiang/xui/widget/imageview/photoview/PhotoVie wAttacher.java com/xuexiang/xui/widget/imageview/preview/view/Bezier BannerView.java com/xuexiang/xui/widget/picker/wheelview/WheelView.ja va com/xuexiang/xui/widget/progress/materialprogressbar/ BaseProgressLayerDrawable.java com/xuexiang/xui/widget/progress/materialprogressbar/ MaterialProgressBar.java com/xuexiang/xui/widget/tabbar/TabSegment.java com/xuexiang/xui/widget/textview/BadgeView.java io/github/inflationx/calligraphy3/ReflectionUtils.java io/github/inflationx/calligraphy3/TypefaceUtils.java io/github/inflationx/calligraphy3/TypefaceUtils.java io/realm/BaseRealm.java io/realm/BaseRealm.java io/realm/RealmConfig.java io/realm/RealmCache.java io/realm/RealmCache.java io/realm/RealmResults.java io/realm/RealmResults.java io/realm/RealmResults.java io/realm/Internal/FinalizerRunnable.java io/realm/Internal/FinalizerRunnable.java io/realm/Internal/CosRealmConfig.java io/realm/internal/CosRealmConfig.java io/realm/internal/CosRealmConfig.java io/realm/internal/RealmCore.java io/realm/internal/CosRealmConfig.java io/realm/internal/CosRealmConfig.java io/realm/internal/CosRealmConfig.java io/realm/internal/CosRealmConfig.java io/realm/internal/CosRealmConfig.java

NO	ISSUE	SEVERITY	STANDARDS	me/jessyan/autosize/DefaultAutoAdaptStrategy.java Fid/jeSsyan/autosize/utils/AutoSizeLog.java org/greenrobot/eventbus/util/ErrorDialogConfig.java
				org/greenrobot/eventbus/util/ErrorDialogManager.java org/greenrobot/eventbus/util/ExceptionToResourceMappi ng.java pub/devrel/easypermissions/EasyPermissions.java pub/devrel/easypermissions/helper/ActivityPermissionHel per.java pub/devrel/easypermissions/helper/BaseSupportPermissi onsHelper.java
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.java cn/finalteam/toolsfinal/StorageUtils.java con/finalteam/toolsfinal/StorageUtils.java com/bosetn/oct16m/kits/Kit.java com/bosetn/oct16m/kits/LFileUtils.java com/bosetn/oct16m/service/LInitService.java com/juphoon/cloud/JCUtils.java com/juphoon/cloud/JCUtils.java com/justalk/cloud/lemon/MtcApi.java com/justalk/cloud/lemon/MtcApi.java com/tencent/bugly/crashreport/common/info/b.java com/yanzhenjie/permission/FileProvider.java com/yanzhenjie/permission/checker/StorageReadTest.jav a com/yanzhenjie/permission/checker/StorageWriteTest.jav a
4	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/bosetn/oct16m/kits/Kit.java com/tencent/bugly/crashreport/common/info/b.java
5	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.java
6	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
7	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.java com/sun/crypto/provider/HmacMD5.java com/sun/crypto/provider/SunJCE_ab.java com/sun/crypto/provider/TlsKeyMaterialGenerator.java com/sun/crypto/provider/TlsMasterSecretGenerator.java com/sun/crypto/provider/TlsPrfGenerator.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	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/DESedeWrapCipher.java com/sun/crypto/provider/HmacPKCS12PBESHA1.java com/sun/crypto/provider/HmacSHA1.java com/sun/crypto/provider/PKCS12PBECipherCore.java com/sun/crypto/provider/TlsKeyMaterialGenerator.java com/sun/crypto/provider/TlsPrfGenerator.java com/tencent/bugly/proguard/z.java
9	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.java com/xuexiang/xui/widget/button/shinebutton/ShineView. java com/xuexiang/xui/widget/textview/badge/BadgeAnimator .java
10	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
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	cn/finalteam/toolsfinal/DeviceUtils.java
12	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
13	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
14	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/CrashReport.java
15	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/HttpsCerManager.java io/socket/engineio/client/transports/PollingXHR.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
16	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.java
17	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

SHARED LIBRARY BINARY ANALYSIS

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.	True info Symbols are stripped.

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.	True info Symbols are 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.	True info Symbols are stripped.

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.	True info Symbols are 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	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.	True info Symbols are stripped.
7	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	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.	True info Symbols are stripped.
9	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	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.	True info Symbols are stripped.

■ NIAP ANALYSIS v1.3

**** *: ABUSED PERMISSIONS**

TYPE	MATCHES	PERMISSIONS
Malware Permissions	19/24	android.permission.CAMERA, android.permission.READ_CALL_LOG, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.INTERNET, android.permission.READ_PHONE_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.GET_TASKS, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.READ_CONTACTS, android.permission.READ_SMS, android.permission.RECEIVE_SMS, android.permission.RECORD_AUDIO, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_WIFI_STATE, android.permission.SYSTEM_ALERT_WINDOW
Other Common Permissions	13/45	android.permission.BROADCAST_STICKY, android.permission.CHANGE_WIFI_STATE, android.permission.PROCESS_OUTGOING_CALLS, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.CALL_PHONE, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.CHANGE_NETWORK_STATE, android.permission.FOREGROUND_SERVICE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.WRITE_CONTACTS, 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
cn-hongkong.log.aliyuncs.com	IP: 47.52.212.53 Country: Hong Kong Region: Hong Kong City: Hong Kong
sts.justalkcloud.com	IP: 122.112.214.251 Country: China Region: Shanghai City: Shanghai
android.bugly.qq.com	IP: 129.226.103.217 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

Q DOMAIN MALWARE CHECK

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

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
sts2.justalkcloud.com	ok	IP: 47.254.65.252 Country: United States of America Region: California City: San Mateo Latitude: 37.547424 Longitude: -122.330589 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
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
sts.justalkcloud.com	ok	IP: 122.112.214.251 Country: China Region: Shanghai City: Shanghai Latitude: 31.222219 Longitude: 121.458061 View: Google Map

DOMAIN	STATUS	GEOLOCATION
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
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
juphoon.com	ok	IP: 106.14.194.67 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 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
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
issuetracker.google.com	ok	IP: 172.217.175.238 Country: Japan Region: Tokyo City: Tokyo Latitude: 35.689507 Longitude: 139.691696 View: Google Map
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
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
realm.io	ok	IP: 18.67.51.103 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
www.googleapis.com	ok	IP: 142.251.42.138 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
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
justalkcloud.com	ok	IP: 122.112.214.251 Country: China Region: Shanghai City: Shanghai Latitude: 31.222219 Longitude: 121.458061 View: Google Map

EMAILS

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

TRACKERS

TRACKER	CATEGORIES	URL
Bugly		https://reports.exodus-privacy.eu.org/trackers/190

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

HARDCODED SECRETS

POSSIBLE SECRETS	
"google_crash_reporting_api_key" : "AlzaSyBjgLrvNK3cf9GAlBOCLYJ79VbSmbULvzQ"	
"google_api_key" : "AlzaSyBjgLrvNK3cf9GAlBOCLYJ79VbSmbULvzQ"	
6e946949562a5cee94987c91ae53162b	
258EAFA5-E914-47DA-95CA-C5AB0DC85B11	
key=AlzaSyAA7vvs7y3G4KL1MMubnHa9RPQ7nsyu3l0	
0123456789abcdefABCDEF	
7065726D697373696F6E40676D61696C2E636F6D	

Report Generated by - MobSF v3.9.5 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.