MOBSF

ANDROID STATIC ANALYSIS REPORT

sonqLgOT (3.0.2)

File Name:	new_pgsHZz.apk
Package Name:	com.bosetn.oct16m
Scan Date:	Nov. 15, 2024, 5:55 a.m.

App Security Score:	46/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
7	34	2	3	6

FILE INFORMATION

File Name: new_pgsHZz.apk
Size: 19.86MB
MD5: 9cfddeedaf1595d42dd689be2ea08e27
SHA1: e8930cb64af879a3331c55a6a30d660d0cb2ab32
SHA256: a0894c98fda1842f1bd8ca9a293f61e2264583c4c48d41aa50605b51e1bf822d

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: 6
Exported Services: 5
Exported Receivers: 7
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=., ST=., O=., OU=., CN=.
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-11-15 05:54:28+00:00
Valid To: 2052-04-02 05:54:28+00:00
Issuer: C=., ST=., O=., OU=., CN=.

Serial Number: 0xdd4fca5dd593c98d
Hash Algorithm: sha384
md5: db2919e12c09b9dfc8d7c05acf54a1f8
sha1: 6e6115f3ccd7e2a8c798a186d0e6d36558d60926
sha256: 9995d618143fc3263dff775d8742c0742b0ce1adb5e1e3d28b574150cd39f25c
sha512: 330d3e736c4e5af9a1e469a9226edf1d1e6ad3254cc90643fe6291de8b1286e1df5bfc306318e305ccc6de3c110b49940c7e41e957a3ac87e560a6ed73b3483e
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b87aaf1814328d8f00e1102b38dcc698affda529f9b7d65ad5a5fbf0f5ed217a
Found 1 unique certificates

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	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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: Compiler — DETAILS: dexlib 2.x

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

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.bosetn.oct16m.CallActivity	Schemes: tel://,
com.bosetn.oct16m.ActionActivity	Schemes: omgodomja://,

ACTIVITY	INTENT
com.bosetn.oct16m.ComPoseActivity	Schemes: sms://, smsto://, mms://, mmsto://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 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.

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.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.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
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.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
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

HIGH: **4** | WARNING: **9** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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
2	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
				cn/finalteam/toolsfinal/logger/AndroidLogTool.java com/bosetn/oct16m/kits/Kit.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bosetn/oct16m/kits/OnlineClientModel.java com/bosetn/oct16m/kits/RandomString.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java 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/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.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/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/executor/GlideExecutor.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java 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/ImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/juphoon/cloud/AndroidAudioManager.java com/juphoon/cloud/JCAccountImpl.java com/juphoon/cloud/JCCallImpl.java com/juphoon/cloud/JCClientImpl.java com/juphoon/cloud/JCDoodleImpl.java com/juphoon/cloud/JCGroupImpl.java com/juphoon/cloud/JCMediaChannelImpl.java com/juphoon/cloud/JCMediaDeviceImpl.java com/juphoon/cloud/JCMediaDeviceVideoCanvas.java com/juphoon/cloud/JCMessageChannelImpl.java com/juphoon/cloud/JCNet.java com/juphoon/cloud/JCPushImpl.java com/juphoon/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.java com/justalk/cloud/zmf/Zmf.java com/justalk/cloud/zmf/ZmfActivity.java com/nonox/tersp/dres/Qesntpa.java com/tencent/bugly/Bugly.java com/tencent/bugly/b.java com/tencent/bugly/crashreport/BuglyLog.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/tencent/bugly/crashreport/CrashReport.java com/tencent/bugly/proguard/f.java com/tencent/bugly/proguard/x.java com/tm/contacts/ContactActivity.java com/tm/contacts/RecentDetailActivity.java com/tm/contacts/adapters/ContactAdapter.java com/tm/contacts/adapters/HomeCallsLogAdapter.java com/tm/contacts/adapters/RecentGroupAdapter.java com/tm/contacts/fragment/ContactsFragment.java com/tm/contacts/fragment/RecentlyFragment.java com/tm/contacts/util/Utils.java com/tm/contacts/viewmodel/ContactViewModel.java com/tm/contacts/viewmodel/DetailViewModel.java com/xuexiang/xui/logs/LogcatLogger.java com/xuexiang/xui/utils/SpanUtils.java com/xuexiang/xui/widget/dialog/bottomsheet/BottomSheet.java com/xuexiang/xui/widget/dialog/materialdialog/internal/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/nine/NineGridImageView.java com/xuexiang/xui/widget/imageview/photoview/PhotoViewAttacher.java com/xuexiang/xui/widget/imageview/preview/view/BezierBannerView.java com/xuexiang/xui/widget/picker/wheelview/WheelView.java com/xuexiang/xui/widget/progress/materialprogressbar/BaseProgressLayerDrawable.java com/xuexiang/xui/widget/progress/materialprogressbar/MaterialProgressBar.java com/xuexiang/xui/widget/spinner/materialspinner/MaterialSpinner.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/viewpump/internal/ReflectionUtils.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	FILES
				io/realm/internal/OsRealmConfig.java io/realm/internal/RealmCore.java io/realm/internal/Util.java
				me/jessyan/autosize/AutoSize.java me/jessyan/autosize/AutoSizeConfig.java me/jessyan/autosize/DefaultAutoAdaptStrategy.java me/jessyan/autosize/utils/AutoSizeLog.java org/greenrobot/eventbus/Logger.java org/greenrobot/eventbus/util/ErrorDialogConfig.java org/greenrobot/eventbus/util/ErrorDialogManager.java org/greenrobot/eventbus/util/ExceptionToResourceMapping.java pub/devrel/easypermissions/EasyPermissions.java pub/devrel/easypermissions/helper/ActivityPermissionHelper.java pub/devrel/easypermissions/helper/BaseSupportPermissionsHelper.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	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 com/bosetn/oct16m/kits/Kit.java com/bosetn/oct16m/kits/LFileUtils.java com/bosetn/oct16m/service/LInitService.java com/juphoon/cloud/JCUtils.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.java com/yanzhenjie/permission/checker/StorageWriteTest.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	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

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	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/manager/RequestManagerRetriever.java com/finalteam2/okhttpfinal/OkHttpTask.java com/juphoon/cloud/JCCallImpl.java com/juphoon/cloud/JCGroupImpl.java com/juphoon/cloud/JCMediaChannel.java com/juphoon/cloud/JCMediaChannelImpl.java com/juphoon/cloud/JCParam.java com/justalk/cloud/avatar/ZpandDevice.java com/justalk/cloud/lemon/MtcApi.java com/justalk/cloud/lemon/MtcBuddyConstants.java com/justalk/cloud/lemon/MtcCallConstants.java com/justalk/cloud/lemon/MtcCcConstants.java com/justalk/cloud/lemon/MtcCliConstants.java com/justalk/cloud/lemon/MtcConf2Constants.java com/justalk/cloud/lemon/MtcConfConstants.java com/justalk/cloud/lemon/MtcContactConstants.java com/justalk/cloud/lemon/MtcDiagConstants.java com/justalk/cloud/lemon/MtcDoodleConstants.java com/justalk/cloud/lemon/MtcFs2Constants.java com/justalk/cloud/lemon/MtcFsConstants.java com/justalk/cloud/lemon/MtcGameConstants.java com/justalk/cloud/lemon/MtcGroupConstants.java com/justalk/cloud/lemon/MtcImConstants.java com/justalk/cloud/lemon/MtcMediaConstants.java com/justalk/cloud/lemon/MtcPathConstants.java com/justalk/cloud/lemon/MtcPaymentConstants.java com/justalk/cloud/lemon/MtcPointConstants.java com/justalk/cloud/lemon/MtcPushConstants.java com/justalk/cloud/lemon/MtcRdCallConstants.java com/justalk/cloud/lemon/MtcRingConstants.java com/justalk/cloud/lemon/MtcSgwConstants.java com/justalk/cloud/lemon/MtcUeConstants.java com/justalk/cloud/lemon/MtcUserConstants.java com/justalk/cloud/lemon/MtcWgwConstants.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	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
11	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
12	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/bosetn/oct16m/kits/MCrypt.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.java com/tencent/bugly/proguard/s.java com/xuexiang/xui/widget/button/shinebutton/ShineView.java com/xuexiang/xui/widget/textview/badge/BadgeAnimator.java
14	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
15	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
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/CrashReport.java
17	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

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	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.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.
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.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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	PIE	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.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.
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.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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	PIE	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.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.
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.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS 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.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.
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.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS 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.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.
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.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	com/juphoon/cloud/MtcEngine.java
00034	Query the current data network type	collection network	cn/finalteam/toolsfinal/DeviceUtils.java com/tencent/bugly/crashreport/common/info/b.java
00013	Read file and put it into a stream	file	cn/finalteam/toolsfinal/io/FileUtils.java com/bosetn/oct16m/kits/Kit.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/getkeepsafe/relinker/elf/ElfParser.java com/juphoon/cloud/JCUtils.java com/justalk/cloud/avatar/ZpandHttp.java com/tencent/bugly/crashreport/common/info/b.java com/tencent/bugly/crashreport/crash/b.java com/tencent/bugly/crashreport/crash/jni/b.java com/tencent/bugly/proguard/n.java com/tencent/bugly/proguard/z.java com/xuexiang/xui/utils/DeviceUtils.java okio/Okio.java
00115	Get last known location of the device	collection location	com/bosetn/oct16m/location/LocService.java
00089	Connect to a URL and receive input stream from the server	command network	cn/finalteam/toolsfinal/io/IOUtils.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/justalk/cloud/avatar/ZpandHttp.java com/tencent/bugly/proguard/s.java io/socket/engineio/client/transports/PollingXHR.java
00094	Connect to a URL and read data from it	command network	cn/finalteam/toolsfinal/io/IOUtils.java com/sun/crypto/provider/SunJCE_b.java io/socket/engineio/client/transports/PollingXHR.java
00108	Read the input stream from given URL	network command	cn/finalteam/toolsfinal/io/IOUtils.java io/socket/engineio/client/transports/PollingXHR.java
00035	Query the list of the installed packages	reflection	cn/finalteam/toolsfinal/ApkUtils.java cn/finalteam/toolsfinal/DeviceUtils.java com/bosetn/oct16m/kits/Kit.java

RULE ID	BEHAVIOUR	LABEL	FILES
00054	Install other APKs from file	reflection	cn/finalteam/toolsfinal/ApkUtils.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	cn/finalteam/toolsfinal/ApkUtils.java cn/finalteam/toolsfinal/DeviceUtils.java com/bosetn/oct16m/MainActivity.java com/bosetn/oct16m/PermissionActivity.java com/bosetn/oct16m/kits/Kit.java com/bosetn/oct16m/receiver/LMSReceiver.java com/bosetn/oct16m/receiver/LSMReceiver.java com/tm/contacts/util/Utils.java
00022	Open a file from given absolute path of the file	file	cn/finalteam/toolsfinal/AppCacheUtils.java cn/finalteam/toolsfinal/CrashHandler.java cn/finalteam/toolsfinal/DeviceUtils.java com/bosetn/oct16m/kits/Kit.java com/bosetn/oct16m/service/LInitService.java com/finalteam2/okhttpfinal/FileDownloadTask.java com/getkeepsafe/relinker/ReLinkerInstance.java com/juphoon/cloud/JCUtils.java com/justalk/cloud/lemon/MtcApi.java com/nonox/tersp/dres/Qesntpa.java com/tencent/bugly/crashreport/crash/anr/b.java com/tencent/bugly/crashreport/crash/jni/NativeCrashHandler.java com/tencent/bugly/crashreport/crash/jni/b.java id/zelory/compressor/ImageUtil.java io/realm/RealmConfiguration.java io/realm/internal/OsRealmConfig.java io/realm/internal/OsSharedRealm.java io/realm/internal/Util.java
00012	Read data and put it into a buffer stream	file	com/justalk/cloud/avatar/ZpandHttp.java com/tencent/bugly/crashreport/crash/jni/b.java
00208	Capture the contents of the device screen	collection screen	com/justalk/cloud/zmf/ScreenCapture.java
00209	Get pixels from the latest rendered image	collection	com/justalk/cloud/zmf/ScreenCapture.java
00096	Connect to a URL and set request method	command network	com/justalk/cloud/avatar/ZpandHttp.java com/tencent/bugly/proguard/s.java io/socket/engineio/client/transports/PollingXHR.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/justalk/cloud/avatar/ZpandHttp.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java com/justalk/cloud/avatar/ZpandHttp.java com/tencent/bugly/proguard/s.java io/socket/engineio/client/transports/PollingXHR.java
00091	Retrieve data from broadcast	collection	com/bosetn/oct16m/receiver/LMSReceiver.java com/bosetn/oct16m/receiver/LSMReceiver.java
00050	Query the SMS service centre timestamp	sms collection	com/bosetn/oct16m/receiver/LMSReceiver.java com/bosetn/oct16m/receiver/LSMReceiver.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bosetn/oct16m/kits/Kit.java com/bosetn/oct16m/service/BaseMessageService.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/yanzhenjie/permission/checker/CalendarReadTest.java com/yanzhenjie/permission/checker/CallLogReadTest.java com/yanzhenjie/permission/checker/ContactsReadTest.java com/yanzhenjie/permission/checker/SmsReadTest.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	cn/finalteam/toolsfinal/BitmapUtils.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	cn/finalteam/toolsfinal/DeviceUtils.java com/justalk/cloud/avatar/ZpandDevice.java
00130	Get the current WIFI information	wifi collection	cn/finalteam/toolsfinal/DeviceUtils.java com/justalk/cloud/avatar/ZpandDevice.java
00033	Query the IMEI number	collection	cn/finalteam/toolsfinal/DeviceUtils.java com/justalk/cloud/avatar/ZpandDevice.java com/yanzhenjie/permission/checker/PhoneStateReadTest.java
00083	Query the IMEI number	collection telephony	cn/finalteam/toolsfinal/DeviceUtils.java
00082	Get the current WiFi MAC address	collection wifi	cn/finalteam/toolsfinal/DeviceUtils.java com/justalk/cloud/avatar/ZpandDevice.java
00102	Set the phone speaker on	command	com/bosetn/oct16m/kits/LCallManager.java com/bosetn/oct16m/service/LCallService.java com/juphoon/cloud/AndroidAudioManager.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/bosetn/oct16m/MainActivity.java com/bosetn/oct16m/PermissionActivity.java com/bosetn/oct16m/kits/Kit.java me/jessyan/autosize/AutoSize.java
00005	Get absolute path of file and put it to JSON object	file	cn/finalteam/toolsfinal/AppCacheUtils.java com/juphoon/cloud/JCUtils.java
00014	Read file into a stream and put it into a JSON object	file	com/juphoon/cloud/JCUtils.java
00121	Create a directory	file command	com/nonox/tersp/dres/Qesntpa.java com/tencent/bugly/proguard/z.java
00125	Check if the given file path exist	file	com/bosetn/oct16m/CallActivity.java com/nonox/tersp/dres/Qesntpa.java com/tencent/bugly/proguard/z.java
00104	Check if the given path is directory	file	com/nonox/tersp/dres/Qesntpa.java
00183	Get current camera parameters and change the setting.	camera	com/justalk/cloud/zmf/CamView.java com/yanzhenjie/permission/checker/CameraTest.java
00131	Get location of the current GSM and put it into JSON	collection location	com/bosetn/oct16m/location/LocManager.java
00099	Get location of the current GSM and put it into JSON	collection location	com/bosetn/oct16m/location/LocManager.java
00016	Get location info of the device and put it to JSON object	location collection	com/bosetn/oct16m/location/LocManager.java
00195	Set the output path of the recorded file	record file	com/bosetn/oct16m/service/LInitService.java
00199	Stop recording and release recording resources	record	com/bosetn/oct16m/service/LInitService.java
00198	Initialize the recorder and start recording	record	com/bosetn/oct16m/service/LInitService.java
00194	Set the audio source (MIC) and recorded file format	record	com/bosetn/oct16m/service/LInitService.java
00197	Set the audio encoder and initialize the recorder	record	com/bosetn/oct16m/service/LInitService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00007	Use absolute path of directory for the output media file path	file	com/bosetn/oct16m/service/LInitService.java
00006	Scheduling recording task	record	com/bosetn/oct16m/service/LInitService.java
00196	Set the recorded file format and output path	record file	com/bosetn/oct16m/service/LInitService.java
00041	Save recorded audio/video to file	record	com/bosetn/oct16m/service/LInitService.java
00112	Get the date of the calendar event	collection calendar	com/alibaba/fastjson/util/TypeUtils.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/bosetn/oct16m/kits/Kit.java com/tm/contacts/util/Utils.java
00106	Get the currently formatted WiFi IP address	collection wifi	com/justalk/cloud/avatar/ZpandNet.java
00189	Get the content of a SMS message	sms	com/bosetn/oct16m/kits/Kit.java com/bosetn/oct16m/service/BaseMessageService.java
00188	Get the address of a SMS message	sms	com/bosetn/oct16m/kits/Kit.java com/bosetn/oct16m/service/BaseMessageService.java
00053	Monitor data identified by a given content URI changes(SMS, MMS, etc.)	sms	com/bosetn/oct16m/service/BaseMessageService.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/bosetn/oct16m/kits/Kit.java com/bosetn/oct16m/service/BaseMessageService.java
00191	Get messages in the SMS inbox	sms	com/bosetn/oct16m/kits/Kit.java com/bosetn/oct16m/service/BaseLogService.java com/bosetn/oct16m/service/BaseMessageService.java
00200	Query data from the contact list	collection contact	com/bosetn/oct16m/kits/Kit.java com/bosetn/oct16m/service/BaseMessageService.java
00187	Query a URI and check the result	collection sms calllog calendar	com/bosetn/oct16m/kits/Kit.java com/bosetn/oct16m/service/BaseMessageService.java
00201	Query data from the call log	collection calllog	com/bosetn/oct16m/kits/Kit.java com/bosetn/oct16m/service/BaseMessageService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00202	Make a phone call	control	com/bosetn/oct16m/kits/Kit.java
00193	Send a SMS message	sms	com/bosetn/oct16m/kits/Kit.java
00038	Query the phone number	collection	com/bosetn/oct16m/kits/Kit.java
00203	Put a phone number into an intent	control	com/bosetn/oct16m/kits/Kit.java
00079	Hide the current app's icon	evasion	com/bosetn/oct16m/kits/Kit.java
00140	Write the phone number into a file	collection telephony file command	com/bosetn/oct16m/kits/Kit.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/bosetn/oct16m/kits/Kit.java
00064	Monitor incoming call status	control	com/bosetn/oct16m/kits/Kit.java
00176	Send sms to a contact of contact list	sms	com/bosetn/oct16m/kits/Kit.java
00161	Perform accessibility service action on accessibility node info	accessibility service	com/bosetn/oct16m/kits/Kit.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/332534704071/namespaces/firebase:fetch?key=AIzaSyBjgLrvNK3cf9GAlBOCLYJ79VbSmbULvzQ. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	19/25	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	13/44	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
android.bugly.qq.com	IP: 14.22.7.140 Country: China Region: Guangdong City: Guangzhou
justalkcloud.com	IP: 60.204.239.85 Country: China Region: Jiangxi City: Nanchang
sts.justalkcloud.com	IP: 60.204.239.85 Country: China Region: Jiangxi City: Nanchang
cn-hongkong.log.aliyuncs.com	IP: 47.90.119.19 Country: Hong Kong Region: Hong Kong City: Hong Kong

DOMAIN	COUNTRY/REGION
juphoon.com	IP: 120.55.165.103 Country: China Region: Zhejiang City: Hangzhou

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
issuetracker.google.com	ok	**IP:** 172.217.25.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
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
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

DOMAIN	STATUS	GEOLOCATION
schemas.android.com	ok	No Geolocation information available.
www.openssl.org	ok	**IP:** 34.49.79.89 **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
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
realm.io	ok	**IP:** 3.170.221.88 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
android.bugly.qq.com	ok	**IP:** 14.22.7.140 **Country:** China **Region:** Guangdong **City:** Guangzhou **Latitude:** 23.116671 **Longitude:** 113.250000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
justalkcloud.com	ok	**IP:** 60.204.239.85 **Country:** China **Region:** Jiangxi **City:** Nanchang **Latitude:** 28.683331 **Longitude:** 115.883331 **View:** Google Map
sts.justalkcloud.com	ok	**IP:** 60.204.239.85 **Country:** China **Region:** Jiangxi **City:** Nanchang **Latitude:** 28.683331 **Longitude:** 115.883331 **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
cn-hongkong.log.aliyuncs.com	ok	**IP:** 47.90.119.19 **Country:** Hong Kong **Region:** Hong Kong **City:** Hong Kong **Latitude:** 22.285521 **Longitude:** 114.157692 **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

DOMAIN	STATUS	GEOLOCATION
www.googleapis.com	ok	**IP:** 172.217.25.170 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
juphoon.com	ok	**IP:** 120.55.165.103 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **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

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

HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyBjgLrvNK3cf9GAlBOCLYJ79VbSmbULvzQ"
"google_crash_reporting_api_key" : "AIzaSyBjgLrvNK3cf9GAlBOCLYJ79VbSmbULvzQ"
7065726D697373696F6E40676D61696C2E636F6D
6e946949562a5cee94987c91ae53162b
key=AIzaSyAA7vvs7y3G4KL1MMubnHa9RPQ7nsyu3l0
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
0123456789abcdefABCDEF

SCAN LOGS

Timestamp	Event	Error
2024-11-15 05:55:40	Generating Hashes	OK
2024-11-15 05:55:40	Extracting APK	OK

2024-11-15 05:55:40	Unzipping	OK
2024-11-15 05:55:40	Getting Hardcoded Certificates/Keystores	OK
2024-11-15 05:55:40	Parsing APK with androguard	OK
2024-11-15 05:55:43	Parsing AndroidManifest.xml	OK
2024-11-15 05:55:43	Extracting Manifest Data	OK
2024-11-15 05:55:43	Performing Static Analysis on: sonqLgOT (com.bosetn.oct16m)	OK
2024-11-15 05:55:43	Fetching Details from Play Store: com.bosetn.oct16m	OK
2024-11-15 05:55:43	Manifest Analysis Started	OK
2024-11-15 05:55:43	Checking for Malware Permissions	OK
2024-11-15 05:55:43	Fetching icon path	OK
2024-11-15 05:55:43	Library Binary Analysis Started	OK
2024-11-15 05:55:43	Analyzing apktool_out/lib/armeabi-v7a/libbbes.so	OK
2024-11-15 05:55:43	Analyzing apktool_out/lib/armeabi-v7a/libBugly.so	OK
2024-11-15 05:55:43	Analyzing apktool_out/lib/armeabi-v7a/libmtc.so	OK

2024-11-15 05:55:44	Analyzing apktool_out/lib/armeabi-v7a/librealm-jni.so	OK
2024-11-15 05:55:44	Analyzing apktool_out/lib/armeabi-v7a/libzmf.so	OK
2024-11-15 05:55:44	Analyzing lib/armeabi-v7a/libbbes.so	OK
2024-11-15 05:55:44	Analyzing lib/armeabi-v7a/libBugly.so	OK
2024-11-15 05:55:44	Analyzing lib/armeabi-v7a/libmtc.so	OK
2024-11-15 05:55:44	Analyzing lib/armeabi-v7a/librealm-jni.so	OK
2024-11-15 05:55:44	Analyzing lib/armeabi-v7a/libzmf.so	OK
2024-11-15 05:55:44	Reading Code Signing Certificate	OK
2024-11-15 05:55:45	Running APKiD 2.1.5	OK
2024-11-15 05:55:49	Updating Trackers Database....	OK
2024-11-15 05:55:49	Detecting Trackers	OK
2024-11-15 05:55:51	Decompiling APK to Java with JADX	OK
2024-11-15 05:56:09	Converting DEX to Smali	OK
2024-11-15 05:56:09	Code Analysis Started on - java_source	OK

2024-11-15 05:56:17	Android SAST Completed	OK
2024-11-15 05:56:17	Android API Analysis Started	OK
2024-11-15 05:56:20	Android API Analysis Completed	OK
2024-11-15 05:56:21	Android Permission Mapping Started	OK
2024-11-15 05:57:18	Android Permission Mapping Completed	OK
2024-11-15 05:57:21	Email and URL Extraction Completed	OK
2024-11-15 05:57:21	Android Behaviour Analysis Started	OK
2024-11-15 05:57:25	Android Behaviour Analysis Completed	OK
2024-11-15 05:57:25	Extracting String data from APK	OK
2024-11-15 05:57:26	Extracting String data from SO	OK
2024-11-15 05:57:26	Extracting String data from Code	OK
2024-11-15 05:57:26	Extracting String values and entropies from Code	OK
2024-11-15 05:57:29	Performing Malware check on extracted domains	OK
2024-11-15 05:57:31	Saving to Database	OK

2024-11-15 06:08:51	Performing Malware check on extracted domains	OK
2024-11-15 06:08:57	Detecting Trackers from Domains	OK

Report Generated by - MobSF v4.1.9

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.