MOBSF

ANDROID STATIC ANALYSIS REPORT

sonqLgOT (3.0.2)

File Name:	newapp.apk
Package Name:	com.bosetn.oct16m
Scan Date:	Nov. 12, 2024, 4:40 a.m.

App Security Score:	45/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
7	34	2	2	1

FILE INFORMATION

File Name: newapp.apk
Size: 19.86MB
MD5: 0189f86586eae9cafe0c53cc60fde0f7
SHA1: 3509b065b21bbf2e22f4ea8e3ff216029ccd57ad
SHA256: 0c776458eda4f503b03822c4eedeba0367125048056765cef8ed7106ae9767b9

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: 2024-11-12 03:51:05+00:00
Valid To: 2052-03-30 03:51:05+00:00
Issuer: C=., ST=., O=., OU=., CN=.

Serial Number: 0x8b1b661743ac5307
Hash Algorithm: sha384
md5: 7877a8ed5ec720a1654c30d87ac8744d
sha1: 1dc8e8ed7d8a111cb864322490a81a9715a3373e
sha256: 3aca071f3f338c6282cf6482c4957ef92c9654f710ca31e63a61d0ff501401e0
sha512: c2c4a04c8c8478a812238a24fdb2507dfe3ec77c5f33f48993865537de41e7a46096f65f601f1623c7a8af2fecc9ca7e9ef9d4dcc6688343c285d1f6306bdbb2
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c1edc95facc7ea9fc05c395d439ac2b20ff05ec0ba7530f530e376c73aa9916a
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	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
				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/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 com/bumptech/glide/load/resource/bitmap/VideoDecode

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	r.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 com/tencent/bugly/crashreport/CrashReport.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				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 io/realm/internal/OsRealmConfig.java io/realm/internal/RealmCore.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				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/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

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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
5	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
6	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
7	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
8	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
9	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
10	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
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

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	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
13	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
14	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
15	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
16	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
17	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

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	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.

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"
0123456789abcdefABCDEF
6e946949562a5cee94987c91ae53162b

POSSIBLE SECRETS
key=AIzaSyAA7vvs7y3G4KL1MMubnHa9RPQ7nsyu3l0
7065726D697373696F6E40676D61696C2E636F6D
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

Report Generated by - MobSF v3.9.8 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.