MOBSF

ANDROID STATIC ANALYSIS REPORT

System Update Service (5.3.4)

File Name:	install_136_1721674928.apk
Package Name:	com.pro.monimaster
Scan Date:	Aug. 10, 2024, 6:59 p.m.

App Security Score: 40/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	22	2	0	4

FILE INFORMATION

File Name: install_136_1721674928.apk
Size: 18.92MB
MD5: b08c5e2fc87ce2c9a9d1f330b09ae61f
SHA1: a7a0cf84867b74d7457c0a01b351a12b083cd849
SHA256: 8b40fb160e28edef4a44824eb665525fc73f23946847f38d145f7961831f0f35

APP INFORMATION

App Name: System Update Service
Package Name: com.pro.monimaster
Main Activity:
Target SDK: 28
Min SDK: 21
Max SDK:
Android Version Name: 5.3.4
Android Version Code: 64

APP COMPONENTS

Activities: 22
Services: 17
Receivers: 11
Providers: 4
Exported Activities: 3
Exported Services: 4
Exported Receivers: 2
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=us, ST=us, L=us, O=monimaster, OU=monimaster, CN=monimaster
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-03-06 01:58:22+00:00
Valid To: 2034-03-04 01:58:22+00:00
Issuer: C=us, ST=us, L=us, O=monimaster, OU=monimaster, CN=monimaster
Serial Number: 0xc779bf17b6b0c4
Hash Algorithm: sha256
md5: 1988334b9ba9a126499c5d55c849267f
sha1: bfb0c1872c08770ff24c0f982de5bc535dd75585

sha256: 56231acf29f9bfc87c33d7d129f9e164baeb994df1e32d381c9d3706d49a2400
sha512: 5e0ea36bfe6b1dfc593f09d9bddb4a14a91b796becb122919fa897b27cb6fa20b52c14671410f00a4e1e322be684891405fdbee621387539161d34422e66febb
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b9433721e01759f5427b1cdd33445c25892f63f6100f41d73cc64d4f867f3ed7
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
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.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.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.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.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.

PERMISSION	STATUS	INFO	DESCRIPTION
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
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.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.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_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.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.ANSWER_PHONE_CALLS	dangerous	permits an app to answer incoming phone calls.	Allows the app to answer an incoming phone call.
android.permission.READ_PHONE_NUMBERS	dangerous	allows reading of the device's phone number(s).	Allows read access to the device's phone number(s). This is a subset of the capabilities granted by READ_PHONE_STATE but is exposed to instant applications.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.BIND_DEVICE_ADMIN	signature	interact with device admin	Allows the holder to send intents to a device administrator. Should never be needed for common applications.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	dangerous	mount and unmount file systems	Allows the application to mount and unmount file systems for removable storage.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

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

FILE	DETAILS
classes2.dex	<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 Build.TAGS check possible VM check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

NETWORK SECURITY

HIGH: **1** | WARNING: **0** | INFO: **0** | SECURE: **0**

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.

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: **11** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
4	Activity-Alias (com.app.pro.service) is not Protected. An intent-filter exists.	warning	An Activity-Alias 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-Alias is explicitly exported.
5	Activity-Alias (com.app.pro.launcher) is not Protected. An intent-filter exists.	warning	An Activity-Alias 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-Alias is explicitly exported.
6	TaskAffinity is set for activity (com.app.pro.activity.FloatGuidePermissionActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
7	Content Provider (com.app.pro.provider.LocalHtmlProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Broadcast Receiver (com.component.permission.service.ComponentAdminService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_DEVICE_ADMIN [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.
9	Service (com.component.permission.service.ComponentNotificationService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_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.component.permission.service.ComponentAccessibilityService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
11	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
12	Activity (com.google.firebase.auth.internal.FederatedSignInActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (28) of the app to 29 or higher to fix this issue at platform level.
13	Activity (com.google.firebase.auth.internal.FederatedSignInActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.firebase.auth.api.gms.permission.LAUNCH_FEDERATED_SIGN_IN [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. 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.
14	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.
15	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **1** | WARNING: **8** | INFO: **2** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/b.java a2/j.java b0/a.java b0/b.java b0/e0.java b0/n0.java b0/s.java b0/v0.java c/a.java com/alibaba/android/arouter/launcher/_ARouter.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/alibaba/android/arouter/AARLaunch/_ARouter.java com/alibaba/android/arouter/utils/ClassUtils.java com/alibaba/android/arouter/utils/DefaultLogger.java com/alibaba/sdk/android/oss/common/OSSLog.java com/alibaba/sdk/android/oss/common/OSSLogToFileUtils.java com/alibaba/sdk/android/oss/common/auth/OSSFederationToken.java com/alibaba/sdk/android/oss/common/utils/HttpdnsMini.java com/alibaba/sdk/android/oss/network/OSSRequestTask.java com/component/permission/activity/InterceptActivity.java com/tencent/mars/xlog/Log.java e0/b.java f/f.java i0/a.java j3/o.java j4/b.java k/c.java k0/a.java k0/c.java k4/a.java l/d.java l/f.java l/h.java l/i.java l/j.java l/l.java l/m.java l/n.java l/o.java l/r.java l/s.java l0/m.java l0/n.java l0/q.java l0/x.java n0/a.java o0/c.java o1/f.java org/java_websocket/AbstractWebSocket.java org/java_websocket/SSLSocketChannel.java org/java_websocket/WebSocketImpl.java org/java_websocket/drafts/Draft_6455.java p/e.java p/f.java p/i.java p0/d.java p3/c.java q0/a.java q3/c.java r/a.java s/e.java s/g.java s0/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t/d.java t/e.java t/f.java t/g.java t/h.java t/m.java u/a.java u/e.java u1/d.java v0/h.java v4/g.java v4/h.java v4/i.java w2/a.java x/g.java x1/a.java
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/alibaba/sdk/android/oss/common/utils/HttpdnsMini.java com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
3	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/alibaba/fastjson/util/AntiCollisionHashMap.java org/java_websocket/drafts/Draft_6455.java t4/f.java
4	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/alibaba/sdk/android/oss/common/utils/BinaryUtil.java org/java_websocket/drafts/Draft_6455.java t4/f.java v4/d.java
5	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	com/alibaba/android/arouter/utils/Consts.java com/alibaba/fastjson/JSON.java t1/a.java
6	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	com/alibaba/sdk/android/oss/common/OSSLogToFileUtils.java com/alibaba/sdk/android/oss/internal/ExtensionRequestOperation.java m1/b.java r1/s.java v4/e.java v4/g.java x1/b.java
7	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	f3/d.java o1/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	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	com/alibaba/sdk/android/oss/common/utils/BinaryUtil.java v4/c.java
9	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and 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/alibaba/sdk/android/oss/common/OSSSQLiteHelper.java p0/c.java
10	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	n2/a.java
11	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	k0/c.java

SHARED LIBRARY BINARY ANALYSIS

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

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
6	arm64-v8a/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__vsnprintf_chk', '__vsprintf_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__read_chk', '__strchr_chk', '__memset_chk']	False warning Symbols are available.
7	arm64-v8a/libmarsxlog.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	arm64-v8a/libWRtcAudio.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__vsprintf_chk']	False warning Symbols are available.
9	armeabi-v7a/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
10	armeabi-v7a/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	armeabi-v7a/libmarsxlog.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
12	armeabi-v7a/libWRtcAudio.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__vsprintf_chk']	False warning Symbols are available.
13	arm64-v8a/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	arm64-v8a/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__vsnprintf_chk', '__vsprintf_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__read_chk', '__strchr_chk', '__memset_chk']	False warning Symbols are available.
15	arm64-v8a/libmarsxlog.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
16	arm64-v8a/libWRtcAudio.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__vsprintf_chk']	False warning Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	16/24	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.READ_PHONE_STATE, android.permission.READ_SMS, android.permission.READ_CONTACTS, android.permission.READ_CALL_LOG, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.RECORD_AUDIO, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.SYSTEM_ALERT_WINDOW, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	13/45	android.permission.CHANGE_WIFI_STATE, android.permission.BLUETOOTH, android.permission.READ_CALENDAR, android.permission.PROCESS_OUTGOING_CALLS, android.permission.CALL_PHONE, android.permission.FOREGROUND_SERVICE, android.permission.BIND_DEVICE_ADMIN, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.BLUETOOTH_ADMIN, android.permission.PACKAGE_USAGE_STATS, android.permission.ACCESS_BACKGROUND_LOCATION, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
oss.aliyuncs.com	IP: 118.178.29.5 Country: China Region: Zhejiang City: Hangzhou
oss-cn-hangzhou.aliyuncs.com	IP: 118.31.219.189 Country: China Region: Zhejiang City: Hangzhou
203.107.1.1	IP: 203.107.1.1 Country: China Region: Zhejiang City: Hangzhou

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
schemas.android.com	ok	No Geolocation information available.
oss-cn-.aliyuncs.comor	ok	No Geolocation information available.
oss.aliyuncs.com	ok	**IP:** 118.178.29.5 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
oss-cn-hangzhou.aliyuncs.com	ok	**IP:** 118.31.219.189 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
203.107.1.1	ok	**IP:** 203.107.1.1 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
lame.sf.net	ok	**IP:** 104.18.21.237 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
image.cnamedomain.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.ietf.org	ok	**IP:** 104.16.44.99 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
127.0.0.1	ok	**IP:** 127.0.0.1 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
aomediacodec.github.io	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
crbug.com	ok	**IP:** 216.239.32.29 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.monimaster.com	ok	**IP:** 163.181.92.232 **Country:** United States of America **Region:** California **City:** San Mateo **Latitude:** 37.547424 **Longitude:** -122.330589 **View:** Google Map
www.webrtc.org	ok	**IP:** 142.250.180.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
appro@openssl.org	lib/arm64-v8a/libjingle_peerconnection_so.so
appro@openssl.org	apktool_out/lib/arm64-v8a/libjingle_peerconnection_so.so

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"permission_google_mail_auth_description" : "□□□□□□Google□□□□□□□□□□ClevGuard□□□□□□□□□□□□□□□□□□□□□□"
"password" : "Palavra-passe"
"authorization_failed" : "□□□□"
"incorrect_password" : "*□□□□□□□□□□□□□□□□□□□□"
"authorization_failed" : "□□□□□□□□□□"
"token_failed" : "□□□□□□□□□□□□□□"
"password" : "Paswoord"
"google_crash_reporting_api_key" : "AIzaSyAY-US0o1dBYeVKTOYXX1XPrOuy-2gA7yk"
"password" : "Contraseña"

POSSIBLE SECRETS
"password" : "□□"
"permission_google_mail_auth_title" : "Gmail□□□□□"
"google_api_key" : "AIzaSyAY-US0o1dBYeVKTOYXX1XPrOuy-2gA7yk"
"key_device" : "kids"
"token_failed" : "□□□□□□□□□□"
"password" : "Passwort"
"permission_google_mail_auth_title" : "Gmail□□"
"com.google.firebase.crashlytics.mapping_file_id" : "7ec4aad9435d4361afe865106cfacf79"
"incorrect_password" : "*□□□□□□□□□"
"password" : "□□□□□"
"password" : "Password"
aHR0cHM6Ly93d3cubW9uaW1hc3Rlci5jb20vcGhvbmUtbW9uaXRvcmluZy1wcmljaW5nLw==
ebf567ce444d77849e435eeb9fc32163
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
cf029002fffdcadf079e8d0a1c9a70ac
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
aHR0cHM6Ly9hY2NvdW50LWFwaS5tb25pbWFzdGVyLmNvbS8=
e08c232712f153ee063660806039ac53
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
470fa2b4ae81cd56ecbcda9735803434cec591fa
8aff2efc47fafe870c738f727dfcfc6e

POSSIBLE SECRETS
22c48b972d4233ebbb5f830d2fbad3ce
e7555de975c1a3b3b1f8c94bb36eafec

SCAN LOGS

Timestamp	Event	Error
2024-08-10 18:59:46	Generating Hashes	OK
2024-08-10 18:59:46	Extracting APK	OK
2024-08-10 18:59:46	Unzipping	OK
2024-08-10 18:59:46	Getting Hardcoded Certificates/Keystores	OK
2024-08-10 18:59:48	Parsing AndroidManifest.xml	OK
2024-08-10 18:59:48	Parsing APK with androguard	OK
2024-08-10 18:59:48	Extracting Manifest Data	OK
2024-08-10 18:59:48	Performing Static Analysis on: System Update Service (com.pro.monimaster)	OK
2024-08-10 18:59:48	Fetching Details from Play Store: com.pro.monimaster	OK
2024-08-10 18:59:49	Manifest Analysis Started	OK

2024-08-10 18:59:49	Reading Network Security config from network_security_config.xml	OK
2024-08-10 18:59:49	Parsing Network Security config	OK
2024-08-10 18:59:49	Checking for Malware Permissions	OK
2024-08-10 18:59:49	Fetching icon path	OK
2024-08-10 18:59:49	Library Binary Analysis Started	OK
2024-08-10 18:59:49	Analyzing lib/armeabi-v7a/libc++_shared.so	OK
2024-08-10 18:59:50	Analyzing lib/armeabi-v7a/libjingle_peerconnection_so.so	OK
2024-08-10 18:59:50	Analyzing lib/armeabi-v7a/libmarsxlog.so	OK
2024-08-10 18:59:50	Analyzing lib/armeabi-v7a/libWRtcAudio.so	OK
2024-08-10 18:59:51	Analyzing lib/arm64-v8a/libc++_shared.so	OK
2024-08-10 18:59:51	Analyzing lib/arm64-v8a/libjingle_peerconnection_so.so	OK
2024-08-10 18:59:52	Analyzing lib/arm64-v8a/libmarsxlog.so	OK
2024-08-10 18:59:52	Analyzing lib/arm64-v8a/libWRtcAudio.so	OK
2024-08-10 18:59:52	Analyzing apktool_out/lib/armeabi-v7a/libc++_shared.so	OK
2024-08-10 18:59:53	Analyzing apktool_out/lib/armeabi-v7a/libjingle_peerconnection_so.so	OK

2024-08-10 18:59:53	Analyzing apktool_out/lib/armeabi-v7a/libmarsxlog.so	OK
2024-08-10 18:59:53	Analyzing apktool_out/lib/armeabi-v7a/libWRtcAudio.so	OK
2024-08-10 18:59:54	Analyzing apktool_out/lib/arm64-v8a/libc++_shared.so	OK
2024-08-10 18:59:55	Analyzing apktool_out/lib/arm64-v8a/libjingle_peerconnection_so.so	OK
2024-08-10 18:59:55	Analyzing apktool_out/lib/arm64-v8a/libmarsxlog.so	OK
2024-08-10 18:59:55	Analyzing apktool_out/lib/arm64-v8a/libWRtcAudio.so	OK
2024-08-10 18:59:55	Reading Code Signing Certificate	OK
2024-08-10 18:59:56	Running APKiD 2.1.5	OK
2024-08-10 18:59:59	Detecting Trackers	OK
2024-08-10 19:00:01	Decompiling APK to Java with jadx	OK
2024-08-10 19:00:22	Converting DEX to Smali	OK
2024-08-10 19:00:22	Code Analysis Started on - java_source	OK
2024-08-10 19:00:35	Android SAST Completed	OK
2024-08-10 19:00:35	Android API Analysis Started	OK
2024-08-10 19:00:43	Android Permission Mapping Started	OK

2024-08-10 19:02:48	Android Permission Mapping Completed	OK
2024-08-10 19:02:50	Finished Code Analysis, Email and URL Extraction	OK
2024-08-10 19:02:50	Extracting String data from APK	OK
2024-08-10 19:02:50	Extracting String data from SO	OK
2024-08-10 19:02:50	Extracting String data from Code	OK
2024-08-10 19:02:50	Extracting String values and entropies from Code	OK
2024-08-10 19:02:52	Performing Malware check on extracted domains	OK
2024-08-10 19:02:55	Saving to Database	OK
