MOBSF

ANDROID STATIC ANALYSIS REPORT

MMGuardian (4.0.14)

File Name:	base.apk
Package Name:	com.mmguardian.childapp
Scan Date:	Aug. 11, 2024, 3:26 p.m.
App Security Score:	45/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	7/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	23	1	1	1

FILE INFORMATION

File Name: base.apk
Size: 40.69MB
MD5: bdcbb8ca26dbcb8ca12122c689898f26
SHA1: 884cb13f3735d4bc7f8168a46e63bddc9dfb3a02
SHA256: 0c90bd528f364cc43b8ca42d2a725f39522be7e03ba227aa5b2a41e556de0657

APP INFORMATION

App Name: MMGuardian
Package Name: com.mmguardian.childapp
Main Activity: com.mmguardian.activity.initial_setup.AdminEntryPointActivity
Target SDK: 33
Min SDK: 26
Max SDK:
Android Version Name: 4.0.14

Android Version Code: 384

APP COMPONENTS

Activities: 77
Services: 31
Receivers: 22
Providers: 5
Exported Activities: 11
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=zheng zhou
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-12-06 05:41:08+00:00
Valid To: 2061-11-23 05:41:08+00:00
Issuer: CN=zheng zhou
Serial Number: 0x4eddaaf4
Hash Algorithm: sha1
md5: 27985904ed434e599262e8ab3e9e5333
sha1: 842933609e604063b55c04bbb47763ac7c0fc327
sha256: e638722c10d395c787298b0d803889c711bf6b00d106bf42cbedc6ae23a199d0
sha512: 7d663fd9d9fafdf7a398e301fa8b0acb6c23c02857d495d3cc2eff6b0641f6bea884ce1bde971c982b81f047fdd39cf7cceb59830dc04fc332f71864ed11a0da
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: c1eecf82f6df09078778d7263af34d2c0eba62acdf194305b2ffea730e1d3c40
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.hardware.telephony	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
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.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.

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_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
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.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
com.android.launcher.permission.INSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.UNINSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.EXPAND_STATUS_BAR	normal	expand/collapse status bar	Allows application to expand or collapse the status bar.
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
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.android.browser.permission.READ_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BIND_NOTIFICATION_LISTENER_SERVICE	signature	required by NotificationListenerServices for system binding.	Must be required by an NotificationListenerService, to ensure that only the system can bind to it.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
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.BIND_ACCESSIBILITY_SERVICE	signature	required by AccessibilityServices for system binding.	Must be required by an AccessibilityService, to ensure that only the system can bind to it.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.BROADCAST_CLOSE_SYSTEM_DIALOGS	unknown	Unknown permission	Unknown permission from android reference
com.mmguardian.permission.PERMISSION1	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.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check FINDINGS: Anti Debug Code — DETAILS: Debug.isDebuggerConnected() check FINDINGS: Compiler — DETAILS: r8

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.mmguardian.safebrowser.SafeBrowserActivity	Schemes: http://, https://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 16 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Activity (com.mmguardian.activity.initial_setup.MessagingAppEntryPointActivity) 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.
3	Activity-Alias (com.mmguardian.activity.initial_setup.MessagingAppYellowEntryPointActivity) is not Protected. [android:exported=true]	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.
4	Activity-Alias (com.mmguardian.activity.initial_setup.MessagingAppRedEntryPointActivity) is not Protected. [android:exported=true]	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.
5	Activity-Alias (com.mmguardian.activity.initial_setup.MessagingAppPurpleEntryPointActivity) is not Protected. [android:exported=true]	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.
6	Activity-Alias (com.mmguardian.activity.initial_setup.MessagingAppOrangeEntryPointActivity) is not Protected. [android:exported=true]	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.
7	Activity-Alias (com.mmguardian.activity.initial_setup.MessagingAppGreenEntryPointActivity) is not Protected. [android:exported=true]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	Activity-Alias (com.mmguardian.activity.initial_setup.MessagingAppBlueEntryPointActivity) is not Protected. [android:exported=true]	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.
9	Activity-Alias (com.mmguardian.activity.initial_setup.MessagingAppBlackEntryPointActivity) is not Protected. [android:exported=true]	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.
10	TaskAffinity is set for activity (com.mmguardian.safebrowser.SafeBrowserActivity)	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.
11	Activity (com.mmguardian.safebrowser.SafeBrowserActivity) 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.
12	Activity (com.mmguardian.activity.LockActivityNew) 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.
13	Activity (com.mmguardian.activity.LockActivityNewAndroidS) 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.
14	Content Provider (com.mmguardian.util.CoreAppContentProvider) is Protected by a permission. Permission: com.mmguardian.permission.PERMISSION2 protectionLevel: signature [android:exported=true]	info	A Content Provider is found to be exported, but is protected by permission.

NO	ISSUE	SEVERITY	DESCRIPTION
15	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.
16	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.
17	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [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.

</> CODE ANALYSIS

HIGH: **2** | WARNING: **6** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a/d/a/a/c.java a/d/b/k/f.java a/f/a/a.java a/h/a/a.java a/i/a/c.java a/j/a.java c/a/a/b/a.java c/b/a/b/i/y/a.java c/b/a/d/a/a.java c/b/a/d/d/c/a6.java c/b/a/d/d/c/c.java c/b/a/d/d/c/f.java c/b/a/d/d/c/k.java c/b/a/d/d/c/l.java c/b/a/d/d/c/m.java c/b/a/d/d/c/m5.java c/b/a/d/d/c/w5.java c/b/a/d/d/f/g.java c/b/a/d/d/f/o2.java c/b/a/d/d/f/y1.java c/b/a/d/d/i/a4.java c/b/a/d/d/i/g.java c/b/a/d/d/i/g3.java c/b/a/d/d/i/h0.java c/b/a/d/d/i/n3.java c/b/a/d/d/i/p3.java c/b/a/d/d/i/u3.java c/b/a/d/d/i/u4.java c/b/a/d/d/i/u5.java c/b/a/d/d/i/v3.java c/b/a/d/d/i/w3.java c/b/a/d/d/i/yb.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive	info	CWE: CWE-532: Insertion of Sensitive	c/b/a/d/d/k/k.java c/b/a/d/d/n/d.java c/b/a/d/d/n/h.java c/b/a/d/d/n/w5.java c/b/a/d/g/a.java c/b/a/d/h/b/a.java com/mmguardian/activity/LockActivity.java com/mmguardian/activity/MonitorActivity.java com/mmguardian/activity/PanicActivity.java com/mmguardian/activity/UninstallProtectionActivity_4_Step.java com/mmguardian/activity/UnlockActivity.java com/mmguardian/activity/UserRegisterationActivity.java com/mmguardian/activity/feature/adultimagedetection/e.java com/mmguardian/activity/feature/app/AdminApplicationContActivity.java com/mmguardian/activity/feature/contact/TypeInNumberActivity.java com/mmguardian/activity/feature/geozone/CreateGeoZoneActivity.java com/mmguardian/activity/feature/lockunlock/b.java com/mmguardian/activity/help/LockAllowedContactsActivity.java com/mmguardian/activity/help/TimeLimitsActivity.java com/mmguardian/activity/help/k.java com/mmguardian/activity/help/m.java com/mmguardian/b/a.java com/mmguardian/b/c.java com/mmguardian/b/d.java com/mmguardian/b/f/b.java com/mmguardian/b/f/c.java com/mmguardian/b/f/d.java com/mmguardian/b/f/e.java com/mmguardian/b/f/f.java com/mmguardian/billing/BillingReceiver.java com/mmguardian/billing/BillingService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
	information should never be logged.	Info	Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/mmguardian/billing/c.java com/mmguardian/billing/h.java com/mmguardian/billing/j/h.java com/mmguardian/broadcaster/DeviceAdminSample.java com/mmguardian/broadcaster/IncomingCallReceiver.java com/mmguardian/broadcaster/LocationTrackingBroadcastReceiver.java com/mmguardian/broadcaster/d.java com/mmguardian/broadcaster/feature/GeoZoneBR.java com/mmguardian/broadcaster/feature/TimeRestControllerBR.java com/mmguardian/c/c.java com/mmguardian/c/p.java com/mmguardian/c/s.java com/mmguardian/dexmodule/thirdpartymon/notificationhelper/BaseNotificationHelper.java com/mmguardian/dexmodule/thirdpartymon/notificationhelper/MessagesNotificationHelper.java com/mmguardian/dexmodule/thirdpartymon/util/MyLogger.java com/mmguardian/h/a.java com/mmguardian/h/e.java com/mmguardian/i/b.java com/mmguardian/j/a/b.java com/mmguardian/j/a/f/d.java com/mmguardian/j/a/h/a.java com/mmguardian/j/a/h/b.java com/mmguardian/j/a/h/c.java com/mmguardian/l/b/a.java com/mmguardian/l/b/b.java com/mmguardian/l/b/c.java com/mmguardian/l/b/f.java com/mmguardian/l/b/g.java com/mmguardian/l/b/h.java com/mmguardian/safebrowser/e.java com/mmguardian/safebrowser/f0.java com/mmguardian/safebrowser/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/mmguardian/safebrowser/g0.java com/mmguardian/safebrowser/k.java com/mmguardian/safebrowser/l.java com/mmguardian/safebrowser/l0.java com/mmguardian/safebrowser/n.java com/mmguardian/safebrowser/o.java com/mmguardian/service/BroadCastReceiverBackendService.java com/mmguardian/service/FeatureMonitorService.java com/mmguardian/service/MonitorService.java com/mmguardian/service/WindowChangeDetectingService.java com/mmguardian/service/b.java com/mmguardian/service/d.java com/mmguardian/util/c0.java com/mmguardian/util/p.java com/mmguardian/view/SwipeRecyclerView.java mmguardian/support/v7/mms/MmsService.java mmguardian/support/v7/mms/f.java mmguardian/support/v7/mms/g.java mmguardian/support/v7/mms/h.java mmguardian/support/v7/mms/i.java mmguardian/support/v7/mms/l.java mmguardian/support/v7/mms/m.java mmguardian/support/v7/mms/n.java mmguardian/support/v7/mms/o.java mmguardian/support/v7/mms/p.java mmguardian/support/v7/mms/r.java mmguardian/support/v7/mms/s/e.java mmguardian/support/v7/mms/s/o.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	a/i/a/g/a.java c/b/a/b/i/a0/j/a0.java c/b/a/b/i/a0/j/r0.java c/b/a/b/i/a0/j/t0.java com/mmguardian/billing/c.java com/mmguardian/d/a.java com/mmguardian/d/b.java com/mmguardian/safebrowser/e.java com/mmguardian/safebrowser/k.java com/mmguardian/safebrowser/l.java com/mmguardian/safebrowser/n.java com/mmguardian/util/CoreAppContentProvider.java
3	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/mmguardian/billing/h.java com/mmguardian/billing/i.java com/mmguardian/billing/j/h.java com/mmguardian/dexmodule/thirdpartymon/service/helper/WhatsAppWindowCallPageHelper.java com/mmguardian/dexmodule/thirdpartymon/util/Util.java com/mmguardian/util/v.java
4	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	com/mmguardian/activity/feature/contact/j.java com/mmguardian/activity/feature/contact/m.java com/mmguardian/activity/phone_app_setup/mmg_phone_wizard/k.java com/mmguardian/activity/wizard/l.java com/mmguardian/activity/wizard/n.java com/mmguardian/c/n.java com/mmguardian/service/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	c/b/a/d/d/i/h0.java com/mmguardian/broadcaster/AppUsageBroadcastReceiver.java com/mmguardian/broadcaster/PowerOffBroadCastReceiver.java com/mmguardian/broadcaster/feature/TimeRestControllerBR.java com/mmguardian/h/c.java com/mmguardian/i/b.java com/mmguardian/safebrowser/f0.java com/mmguardian/safebrowser/h0.java
6	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/mmguardian/util/n.java
7	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/mmguardian/activity/feature/webfilter/UrlToCategoryMappings.java com/mmguardian/bo/PendingCommandsToServerList.java com/mmguardian/dexmodule/AnalyzeTextCategory.java com/mmguardian/dexmodule/thirdpartymon/service/helper/GoogleMessagesHelper.java com/mmguardian/dexmodule/thirdpartymon/util/AppsStringDataUtils.java
8	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/mmguardian/j/a/g/a.java com/mmguardian/safebrowser/h0.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	c/b/a/d/d/i/a4.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/mmguardian/activity/feature/app/appcontrol3/ApplicationController3Activity.java com/mmguardian/c/s.java com/mmguardian/service/d.java

SHARED LIBRARY BINARY ANALYSIS

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	mips64/libbdpush_V2_6.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/libtensorflowlite_jni.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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	armeabi-v7a/libbdpush_V2_6.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86_64/libtensorflowlite_jni.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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	x86_64/libbdpush_V2_6.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	arm64-v8a/libtensorflowlite_jni.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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	arm64-v8a/libbdpush_V2_6.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	x86/libtensorflowlite_jni.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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	x86/libbdpush_V2_6.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	armeabi/libbdpush_V2_6.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	mips/libbdpush_V2_6.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	mips64/libbdpush_V2_6.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	armeabi-v7a/libtensorflowlite_jni.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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	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	armeabi-v7a/libbdpush_V2_6.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
15	x86_64/libtensorflowlite_jni.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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	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
16	x86_64/libbdpush_V2_6.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
17	arm64-v8a/libtensorflowlite_jni.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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	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
18	arm64-v8a/libbdpush_V2_6.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
19	x86/libtensorflowlite_jni.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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	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
20	x86/libbdpush_V2_6.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
21	armeabi/libbdpush_V2_6.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
22	mips/libbdpush_V2_6.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	15/24	android.permission.READ_CONTACTS, android.permission.READ_PHONE_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.VIBRATE, android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.GET_TASKS, android.permission.SYSTEM_ALERT_WINDOW
Other Common Permissions	12/45	android.permission.MODIFY_AUDIO_SETTINGS, android.permission.WRITE_CONTACTS, android.permission.CALL_PHONE, android.permission.CHANGE_WIFI_STATE, android.permission.CHANGE_NETWORK_STATE, android.permission.ACCESS_BACKGROUND_LOCATION, com.android.launcher.permission.INSTALL_SHORTCUT, android.permission.FOREGROUND_SERVICE, android.permission.PACKAGE_USAGE_STATS, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

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

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
thor.komodia.com	ok	**IP:** 207.182.136.170 **Country:** United States of America **Region:** Ohio **City:** Columbus **Latitude:** 40.079235 **Longitude:** -82.940567 **View:** Google Map
api-project-321561395509.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
rodimus.komodia.com	ok	**IP:** 223.252.24.17 **Country:** Australia **Region:** New South Wales **City:** Tuggerah **Latitude:** -33.316669 **Longitude:** 151.416672 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
google.com	ok	**IP:** 142.250.180.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.facebook.com	ok	**IP:** 157.240.234.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
maps.google.com	ok	**IP:** 142.250.180.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
optimus.komodia.com	ok	**IP:** 78.110.173.202 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	ok	**IP:** 142.251.208.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.youtube.com	ok	**IP:** 142.251.208.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
family.mmguardian.com	ok	**IP:** 142.251.39.83 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
zt68s.app.goo.gl	ok	**IP:** 142.251.208.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app-measurement.com	ok	**IP:** 142.250.180.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
portal.mmguardian.com	ok	**IP:** 142.251.39.83 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.mmguardian.com	ok	**IP:** 104.16.151.108 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
play.google.com	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

DOMAIN	STATUS	GEOLOCATION
www.gstatic.com	ok	**IP:** 142.250.180.227 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://api-project-321561395509.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
sales@mmguardian.com	com/mmguardian/c/e0.java
gptest@mmguardian.com	com/mmguardian/service/d.java
support@mmguardian.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

HARDCODED SECRETS

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyCD6-onx84U2NrBm_AAwkeu74cZXOteULQ"
"adminPassword" : "□□□□□□"
"regPassword" : "Senha"

POSSIBLE SECRETS
"mms_messaging_category_pref_key" : "mms_messaging_category"
"notification_reset_pref_key" : "notification_reset"
"notifications_group_children_key" : "notifications_group_children"
"notification_vibration_pref_key" : "notification_vibration"
"mms_phone_number_pref_key" : "buglesub_mms_phone_number"
"userName" : "□□□□□□□□"
"use_local_apn_pref_key" : "use_local_apn_pref_key"
"notifications_category_pref_key" : "notifications_category"
"group_mms_pref_key" : "buglesub_group_messaging"
"sms_enabled_pref_key" : "sms_enabled"
"superlock_enabled_password" : "□□□□□□□"
"messenger_color_theme_pref_key" : "messenger_color_theme_pref_key"
"superlock_enter_kids_password" : "□□□□□□□□□□□□□□□□□□□□□□□□□□"
"changeAdminPassword" : "□□□□□□□□"
"dump_mms_pref_key" : "dump_mms"

POSSIBLE SECRETS
"notification_sound_pref_key" : "notification_sound"
"show_password" : "□□□□□□□□□□□□"
"auto_retrieve_mms_pref_key" : "buglesub_auto_retrieve_mms"
"regPassword" : "contraseña"
"debug_pref_key" : "debug_category"
"advanced_category_pref_key" : "advanced_category"
"auto_retrieve_mms_when_roaming_pref_key" : "buglesub_auto_retrieve_mms_when_roaming"
"superlock_disabled_does_not_remove_password" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□,□□□□□□□□□□□□□□□□□□□□□□"
"notifications_enabled_pref_key" : "notifications_enabled"
"messenger_icon_color_pref_key" : "messenger_icon_color_pref_key"
"contacts_file_provider_authority" : "com.mmguardian.dialer.files"
"delivery_reports_pref_key" : "buglesub_delivery_reports"
"advanced_pref_key" : "advanced_prefs"
"superlock_no_kids_password" : "□□□□□□□□□□□□"
"firebase_database_url" : "https://api-project-321561395509.firebaseio.com"

POSSIBLE SECRETS
"sms_disabled_pref_key" : "sms_disabled"
"wireless_alerts_key" : "buglesub_wireless_alerts_key"
"sms_apns_key" : "sms_apns_key"
"dump_sms_pref_key" : "dump_sms"
"regPassword" : "Password"
"apn_list_pref_key" : "buglesub_apn_list"
"regPassword" : "□□"
"send_sound_pref_key" : "send_sound"
"google_api_key" : "AIzaSyCD6-onx84U2NrBm_AAwkeu74cZXOteULQ"
5e8f16062ea3cd2c4a0d547876baa6f38cabf625
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
123456789009876543211234567890 12
9b8f518b086098de3d77736f9458a3d2f6f95a37
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
8a3c4b262d721acd49a4bf97d5213199c86fa2b9

POSSIBLE SECRETS
cc2751449a350f668590264ed76692694a80308a
c103703e120ae8cc73c9248622f3cd1e
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
470fa2b4ae81cd56ecbcda9735803434cec591fa
49f946663a8deb7054212b8adda248c6

PLAYSTORE INFORMATION

Title: MMGuardian Child Phone App

Score: 1.7852942 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Tools **Play Store URL:** com.mmguardian.childapp

Developer Details: MMGuardian.com, 6277956700908348398, 78 John Miller Way, Suite 326-HD, Kearny NJ 07032, https://www.mmguardian.com?utm_source=playstore&utm_medium=referral&utm_content=parental_control_new, support@mmguardian.com,

Release Date: Dec 5, 2014 **Privacy Policy:** Privacy link

Description:

MMGuardian Parental Control app gives parents the ability to set up parental control and us AI to monitor inappropriate pictures, social media, websites, location and much more. MMGuardian helps parents to protect their child from: * cyber predators(grooming, sextortion) * cyberbullying * drug abuse * violence * suicide ideation * sexting and stay in the know about their phone usage habits. Parents can set up comprehensive parental controls and monitoring on their child's Android phone. MMGuardian can also monitor picture messages, soical media messages, apps, contacts among other parental control features. Note: The app uses Android AccessibilityService API to implement some of the core features: 1. It collects App Usage Data to enable app monitoring and app blocking. 2. It collects Web Browsing History to implement web filtering and monitor. 3. It collects selected Social Media Message Data to implement child safety alerts and message reports on popular messaging apps. MMGuardian is a monitoring app for parents to keep their kids safe, and shall not be used to monitor anyone else even with their permission. MMGuardian is not a spying app. How To Keep Your Teen Safe • Download the MMGuardian Parental Control App to your child’s smartphone, and launch the app. • Register the app, and follow the in-app guidance to set up the app. • Configure the functions to your requirements and receive reports at the MMGuardian Parent Web Portal or the dedicated Parent App app for the parent's phone: https://play.google.com/store/apps/details?id=com.mmguardian.parentapp The app includes a range of Parental Control functions specifically designed for parents to be able to: ★ Take advantage of the latest advances in Artificial Intelligence (AI) to be alerted when a

potentially inappropriate image is detected as having been exchanged in an MMS picture message, or stored on your child’s phone. ★ Receive specific alerts when the content of your child’s social chat messages may indicate cyberbullying, violence, suicidal thoughts, and more. Additional Functions The MMGuardian Parental Control app also includes optional functions enabling parents to: Locate your child’s phone Block and monitor phone calls Limit screen time with a comprehensive App Control function Lock the phone at pre-defined times Enforce safe browsing with an advanced Web Filtering function. Uninstall Protection • The MMGuardian Uninstall Protection function hinders kids from removing or tampering with the app. • If Uninstall Protection function has been enabled, the app's Device Administrator status must first be disabled in order to uninstall the app. • To uninstall the app the easy way: open the app, enter your parent admin password and tap on the trash can icon at the top. Watch our video on YouTube for how to install and register the app on your child's phone: https://youtu.be/6CiZlvs9ObY Free 14 Day Trial All features are fully functional for the free 14-day trial period, after which continued use requires a subscription or license to be purchased. No purchase is required to activate the free trial. Single phone subscriptions are available at USD $4.99 monthly or USD $49.99 annually. Family plans covering up to 5 devices are available at twice the single phone price. Download today and help keep your teen safe with MMGuardian. PLEASE NOTE: This app uses the Device Administrator permission. This app uses Accessibility Service. This app uses Location "in the background" (when the app is not open) so that parents may obtain the location of their child's phone. For more information please visit our website: https://www.mmguardian.com

SCAN LOGS

Timestamp	Event	Error
2024-08-11 15:26:33	Generating Hashes	OK
2024-08-11 15:26:33	Extracting APK	OK
2024-08-11 15:26:33	Unzipping	OK
2024-08-11 15:26:33	Getting Hardcoded Certificates/Keystores	OK
2024-08-11 15:26:36	Parsing AndroidManifest.xml	OK

2024-08-11 15:26:36	Parsing APK with androguard	OK
2024-08-11 15:26:37	Extracting Manifest Data	OK
2024-08-11 15:26:37	Performing Static Analysis on: MMGuardian (com.mmguardian.childapp)	OK
2024-08-11 15:26:37	Fetching Details from Play Store: com.mmguardian.childapp	OK
2024-08-11 15:26:37	Manifest Analysis Started	OK
2024-08-11 15:26:37	Checking for Malware Permissions	OK
2024-08-11 15:26:37	Fetching icon path	OK
2024-08-11 15:26:37	Library Binary Analysis Started	OK
2024-08-11 15:26:37	Analyzing lib/mips64/libbdpush_V2_6.so	OK
2024-08-11 15:26:38	Analyzing lib/armeabi-v7a/libtensorflowlite_jni.so	OK
2024-08-11 15:26:38	Analyzing lib/armeabi-v7a/libbdpush_V2_6.so	OK

2024-08-11 15:26:38	Analyzing lib/x86_64/libtensorflowlite_jni.so	OK
2024-08-11 15:26:38	Analyzing lib/x86_64/libbdpush_V2_6.so	OK
2024-08-11 15:26:38	Analyzing lib/arm64-v8a/libtensorflowlite_jni.so	OK
2024-08-11 15:26:38	Analyzing lib/arm64-v8a/libbdpush_V2_6.so	OK
2024-08-11 15:26:38	Analyzing lib/x86/libtensorflowlite_jni.so	OK
2024-08-11 15:26:38	Analyzing lib/x86/libbdpush_V2_6.so	OK
2024-08-11 15:26:38	Analyzing lib/armeabi/libbdpush_V2_6.so	OK
2024-08-11 15:26:38	Analyzing lib/mips/libbdpush_V2_6.so	OK
2024-08-11 15:26:38	Analyzing apktool_out/lib/mips64/libbdpush_V2_6.so	OK
2024-08-11 15:26:39	Analyzing apktool_out/lib/armeabi-v7a/libtensorflowlite_jni.so	OK
2024-08-11 15:26:39	Analyzing apktool_out/lib/armeabi-v7a/libbdpush_V2_6.so	OK

2024-08-11 15:26:39	Analyzing apktool_out/lib/x86_64/libtensorflowlite_jni.so	OK
2024-08-11 15:26:39	Analyzing apktool_out/lib/x86_64/libbdpush_V2_6.so	OK
2024-08-11 15:26:39	Analyzing apktool_out/lib/arm64-v8a/libtensorflowlite_jni.so	OK
2024-08-11 15:26:39	Analyzing apktool_out/lib/arm64-v8a/libbdpush_V2_6.so	OK
2024-08-11 15:26:39	Analyzing apktool_out/lib/x86/libtensorflowlite_jni.so	OK
2024-08-11 15:26:39	Analyzing apktool_out/lib/x86/libbdpush_V2_6.so	OK
2024-08-11 15:26:39	Analyzing apktool_out/lib/armeabi/libbdpush_V2_6.so	OK
2024-08-11 15:26:39	Analyzing apktool_out/lib/mips/libbdpush_V2_6.so	OK
2024-08-11 15:26:39	Reading Code Signing Certificate	OK
2024-08-11 15:26:40	Running APKiD 2.1.5	OK
2024-08-11 15:26:42	Detecting Trackers	OK

2024-08-11 15:26:43	Decompiling APK to Java with jadx	OK
2024-08-11 15:27:00	Converting DEX to Smali	OK
2024-08-11 15:27:00	Code Analysis Started on - java_source	OK
2024-08-11 15:27:18	Android SAST Completed	OK
2024-08-11 15:27:18	Android API Analysis Started	OK
2024-08-11 15:27:36	Android Permission Mapping Started	OK
2024-08-11 15:28:13	Android Permission Mapping Completed	OK
2024-08-11 15:28:18	Finished Code Analysis, Email and URL Extraction	OK
2024-08-11 15:28:18	Extracting String data from APK	OK
2024-08-11 15:28:20	Extracting String data from SO	OK
2024-08-11 15:28:20	Extracting String data from Code	OK

2024-08-11 15:28:20	Extracting String values and entropies from Code	OK
2024-08-11 15:28:25	Performing Malware check on extracted domains	OK
2024-08-11 15:28:28	Saving to Database	OK

Report Generated by - MobSF v4.0.6

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.