MobSF

ANDROID STATIC ANALYSIS REPORT

Android Service (1.7.0)

File Name:	cm-kids.apk
Package Name:	com.android.settings.app
Scan Date:	Aug. 15, 2024, 7:51 p.m.

App Security Score:	53/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	28	1	3	1

FILE INFORMATION

File Name: cm-kids.apk

Size: 3.32MB

MD5: 4df3c02735375ccfe2662b2356af592a

SHA1: f8ef821e5f86e71e55d7037bc91fdb9ba8370ee8

SHA256: 316a1ded1dccf912f4fd91dc8c1ef05441d1cad739a1ad79c3783916aef4d53f

APP INFORMATION

App Name: Android Service

Package Name: com.android.settings.app

Main Activity:

Target SDK: 23

Min SDK: 17

Max SDK:

Android Version Name: 1.7.0

Android Version Code: 70

APP COMPONENTS

Activities: 9

Services: 49

Receivers: 16

Providers: 2

Exported Activities: 2

Exported Services: 6

Exported Receivers: 11

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: True

v2 signature: True

v3 signature: False

v4 signature: False

X.509 Subject: C=91, ST=Delhi, L=IN, O=Cyberro, OU=Cyberro Technologies, CN=Chyld Monitor

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2020-12-05 08:07:04+00:00

Valid To: 2045-11-29 08:07:04+00:00

Issuer: C=91, ST=Delhi, L=IN, O=Cyberro, OU=Cyberro Technologies, CN=Chyld Monitor

Serial Number: 0x6100b283

Hash Algorithm: sha256

md5: 505ef8f007df29c9ac66e8a2be770bd9

sha1: e7d395df3b8077c733d9be67d841fdf271f49406

sha256: 610d63db0c3c134a9c668bbc53fc6dc34d86a4a9860a3ac178c9371289a675f5

```
sha512: 7097690a1f2b5df1598329c046ec4b99263ba0cf12cfa30d981cbdc305a89cced8b80119b96b05a0f178c4053e557d99560dfb645b789a5730a4bdf0a0df1f3c
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: a5aadd1ff14dfc5c5ac20432a942ccdc2d9b55b0aa5519772ab4829165b92bc6
Found 1 unique certificates
```

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.
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.ACCESS_SUPERUSER	unknown	Unknown permission	Unknown permission from android reference
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.ANSWER_PHONE_CALLS	dangerous	permits an app to answer incoming phone calls.	Allows the app to answer an incoming phone call.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
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.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.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_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_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_HISTORY_BOOKMARKS	dangerous	read Browser's history and bookmarks	Allows the application to read all the URLs that the browser has visited and all of the browser's bookmarks.
android.permission.READ_LOGS	dangerous	read sensitive log data	Allows an application to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information.

PERMISSION	STATUS	INFO	DESCRIPTION
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_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
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.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
com.android.browser.permission.READ_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.android.settings.app.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr><tr><td>Compiler</td><td>r8</td></tr></table></td></tr>
<tr><td>res/raw/module.zip!system/priv-app/PhotosViewer2/PhotosViewer2.apk!classes.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table></td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

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

MANIFEST ANALYSIS

HIGH: **2** | WARNING: **20** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.2-4.2.2, [minSdk=17]	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	Activity-Alias (com.android.settings.app.Launcher2Activity) 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.
4	Activity-Alias (com.android.settings.app.LauncherActivity) 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	Broadcast Receiver (com.android.settings.app.receivers.BatteryLevelReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
6	Broadcast Receiver (com.android.settings.app.receivers.BootCompletedReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
7	Broadcast Receiver (com.android.settings.app.receivers.ConnectivityReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
8	Broadcast Receiver (com.android.settings.app.receivers.DeviceAdministrationReceiver) 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	Broadcast Receiver (com.android.settings.app.receivers.PackageChangedReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
10	Broadcast Receiver (com.android.settings.app.receivers.PhoneStateReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
11	Broadcast Receiver (com.android.settings.app.receivers.PowerConnectionReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
12	Broadcast Receiver (com.android.settings.app.receivers.SensorsChangedReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
13	Broadcast Receiver (com.android.settings.app.receivers.SimChangedReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
14	Broadcast Receiver (com.android.settings.app.receivers.UserPresentReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
15	Service (com.android.settings.app.services.FirebaseInstanceIDService) is not Protected. An intent-filter exists.	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.
16	Service (com.android.settings.app.services.FirebaseMessageService) is not Protected. An intent-filter exists.	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.
17	Service (com.android.settings.app.services.NotificationService) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
18	Service (com.android.settings.app.services.ScreenReaderService) 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.
19	Service (com.google.firebase.messaging.FirebaseMessagingService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
20	Broadcast Receiver (com.google.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.
21	Service (com.google.firebase.iid.FirebaseInstanceIdService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
22	High Intent Priority (1000) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c/a/b/c.java c/a/c/a/c.java c/a/c/a/f/b.java c/a/c/b/d.java c/a/c/b/e.java c/b/d/a/h.java c/b/e/g0.java c/b/e/h0.java c/b/e/m0.java c/b/e/p0.java c/b/e/q0.java c/b/e/r0.java c/b/f/a/i.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	c/b/f/a/n.java c/b/f/b/c.java c/b/f/c/b.java c/b/f/c/c.java c/b/f/c/e.java c/b/f/c/f.java c/b/f/c/i/e.java c/b/f/h/e.java c/b/f/i/d.java c/b/f/i/e.java c/b/f/i/o.java c/b/f/i/q.java c/b/f/j/c.java c/b/f/j/e.java c/b/f/j/j.java c/b/f/j/p.java c/b/g/a/h.java c/b/g/a/m.java c/b/g/a/p.java c/b/g/a/y.java c/b/g/c/a/a.java c/b/g/f/f.java c/b/g/f/i/e.java c/b/g/f/i/h.java c/b/g/g/a1.java c/b/g/g/c0.java c/b/g/g/c2.java c/b/g/g/f1.java c/b/g/g/l.java c/b/g/g/n1.java c/b/g/g/t1.java c/b/g/g/w1.java c/b/g/g/x1.java c/b/g/g/y.java c/b/g/g/y0.java e/a/a/a/z/h.java e/b/e.java e/c/a/a/a.java e/c/a/a/d/h.java e/c/a/a/e/b.java e/c/a/a/e/c.java e/d/a/a/b/c.java e/d/a/a/b/f/k/b2.java e/d/a/a/b/f/k/c0.java e/d/a/a/b/f/k/e0.java e/d/a/a/b/f/k/f2.java e/d/a/a/b/f/k/g.java e/d/a/a/b/f/k/j0.java e/d/a/a/b/f/k/k1.java e/d/a/a/b/f/k/l0.java e/d/a/a/b/f/k/p.java e/d/a/a/b/f/k/x.java e/d/a/a/b/f/k/z1.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				e/d/a/a/b/f/k/z1.java e/d/a/a/b/g/a.java e/d/a/a/b/g/b0.java e/d/a/a/b/g/e.java e/d/a/a/b/g/g0.java e/d/a/a/b/g/i.java e/d/a/a/b/g/k0.java e/d/a/a/b/g/q0.java e/d/a/a/b/g/r.java e/d/a/a/b/g/v0.java e/d/a/a/b/g/w0.java e/d/a/a/b/h/a.java e/d/a/a/b/o.java e/d/a/a/b/u.java e/d/a/a/b/v.java e/d/a/a/f/k1.java e/d/a/a/f/n0.java e/d/a/a/f/o0.java e/d/b/a.java e/d/b/c/a.java e/d/b/c/d.java e/d/b/c/e.java e/d/b/c/f.java e/d/b/c/g.java e/d/b/c/h.java e/d/b/c/j.java e/d/b/c/k.java e/d/b/c/l.java e/d/b/c/m.java e/d/b/c/o.java e/d/b/c/p.java e/d/b/c/q.java e/d/b/d/c.java e/d/b/e.java e/e/a/a.java e/e/a/b.java e/e/a/f/a.java e/e/a/g/a/c.java e/e/a/g/b/a.java e/e/a/g/c/a.java e/e/a/i/c.java e/e/b/a/a.java e/f/a/d/m.java h/a/a/e.java h/a/a/f.java k/b/a/a/a/a.java k/b/a/b/a/v/b.java k/b/a/b/a/v/c.java net/callrec/library/fix/CallRecorderFixHelper.java net/callrec/library/fix/LibLoader.java org/eclipse/paho/android/service/MqttService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	c/a/c/b/e.java c/b/f/b/a.java org/eclipse/paho/android/service/MqttService.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	i/x.java k/b/a/b/a/v/s/a.java
4	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	e/a/a/a/z/f.java e/c/a/a/e/b.java e/d/b/c/j.java
5	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	c/a/c/a/f/b.java c/a/c/b/d.java k/b/a/a/a/c.java
6	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	e/a/a/a/z/g.java
7	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	e/a/a/a/z/g.java
8	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	e/d/b/c/j.java k/b/a/b/a/v/t/d.java
9	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	c/a/c/b/e.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	armeabi-v7a/libCallRecFix.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.
2	x86_64/libCallRecFix.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	arm64-v8a/libCallRecFix.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/libCallRecFix.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.
5	armeabi-v7a/libCallRecFix.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	x86_64/libCallRecFix.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
7	arm64-v8a/libCallRecFix.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.
8	x86/libCallRecFix.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.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	17/24	android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.CAMERA, android.permission.GET_ACCOUNTS, android.permission.INTERNET, android.permission.READ_CALL_LOG, android.permission.READ_CONTACTS, android.permission.READ_EXTERNAL_STORAGE, android.permission.READ_PHONE_STATE, android.permission.READ_SMS, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECORD_AUDIO, android.permission.SYSTEM_ALERT_WINDOW, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE
Other Common Permissions	14/45	android.permission.READ_CALENDAR, android.permission.ACCESS_SUPERUSER, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.CALL_PHONE, android.permission.CHANGE_WIFI_STATE, android.permission.FOREGROUND_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.PACKAGE_USAGE_STATS, android.permission.PROCESS_OUTGOING_CALLS, android.permission.REQUEST_INSTALL_PACKAGES, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, com.google.android.gms.permission.ACTIVITY_RECOGNITION, com.google.android.c2dm.permission.RECEIVE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
pixplicity.com	ok	**IP:** 149.210.244.141 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
google.com	ok	**IP:** 142.251.36.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
android.chyldmonitor.com	ok	**IP:** 18.219.40.56 **Country:** United States of America **Region:** Ohio **City:** Columbus **Latitude:** 39.961182 **Longitude:** -82.998787 **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
plus.google.com	ok	**IP:** 142.251.36.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

✉ EMAILS

EMAIL	FILE
u0013android@android.com u0013android@android.com0	e/d/a/a/b/t.java

HARDCODED SECRETS

POSSIBLE SECRETS
"default_password" : "$654321#"
"google_api_key" : "AIzaSyCCl9bqlgY24dVXGcgya0eWbegmzbvunzw"
"google_crash_reporting_api_key" : "AIzaSyCCl9bqlgY24dVXGcgya0eWbegmzbvunzw"
"library_easypreferences_authorWebsite" : "http://pixplicity.com"
"library_easypreferences_author" : "Pixplicity"
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
af8bc14dc5b1eece9f263a0b9e8e98d0
112d093013cbc36da6762544235aa053

SCAN LOGS

Timestamp	Event	Error
2024-08-15 19:51:00	Generating Hashes	OK
2024-08-15 19:51:00	Extracting APK	OK
2024-08-15 19:51:01	Unzipping	OK
2024-08-15 19:51:03	Getting Hardcoded Certificates/Keystores	OK
2024-08-15 19:51:14	Parsing AndroidManifest.xml	OK

2024-08-15 19:51:14	Parsing APK with androguard	OK
2024-08-15 19:51:15	Extracting Manifest Data	OK
2024-08-15 19:51:15	Performing Static Analysis on: Android Service (com.android.settings.app)	OK
2024-08-15 19:51:15	Fetching Details from Play Store: com.android.settings.app	OK
2024-08-15 19:51:15	Manifest Analysis Started	OK
2024-08-15 19:51:15	Checking for Malware Permissions	OK
2024-08-15 19:51:16	Fetching icon path	OK
2024-08-15 19:51:16	Library Binary Analysis Started	OK
2024-08-15 19:51:16	Analyzing lib/armeabi-v7a/libCallRecFix.so	OK
2024-08-15 19:51:18	Analyzing lib/x86_64/libCallRecFix.so	OK
2024-08-15 19:51:21	Analyzing lib/arm64-v8a/libCallRecFix.so	OK
2024-08-15 19:51:23	Analyzing lib/x86/libCallRecFix.so	OK
2024-08-15 19:51:27	Analyzing apktool_out/lib/armeabi-v7a/libCallRecFix.so	OK
2024-08-15 19:51:29	Analyzing apktool_out/lib/x86_64/libCallRecFix.so	OK

2024-08-15 19:51:33	Analyzing apktool_out/lib/arm64-v8a/libCallRecFix.so	OK
2024-08-15 19:51:35	Analyzing apktool_out/lib/x86/libCallRecFix.so	OK
2024-08-15 19:51:38	Reading Code Signing Certificate	OK
2024-08-15 19:51:41	Running APKiD 2.1.5	OK
2024-08-15 19:51:45	Detecting Trackers	OK
2024-08-15 19:51:47	Decompiling APK to Java with jadx	OK
2024-08-15 19:52:03	Converting DEX to Smali	OK
2024-08-15 19:52:03	Code Analysis Started on - java_source	OK
2024-08-15 19:52:15	Android SAST Completed	OK
2024-08-15 19:52:15	Android API Analysis Started	OK
2024-08-15 19:52:24	Android Permission Mapping Started	OK
2024-08-15 19:52:56	Android Permission Mapping Completed	OK
2024-08-15 19:52:58	Finished Code Analysis, Email and URL Extraction	OK
2024-08-15 19:52:58	Extracting String data from APK	OK

2024-08-15 19:52:58	Extracting String data from SO	OK
2024-08-15 19:52:58	Extracting String data from Code	OK
2024-08-15 19:52:58	Extracting String values and entropies from Code	OK
2024-08-15 19:52:59	Performing Malware check on extracted domains	OK
2024-08-15 19:53:01	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.