

ANDROID STATIC ANALYSIS REPORT



Sync Services (5.3.3)

File Name: 5009_5.3.3_3877.apk

Package Name: com.fp.backup

Scan Date: Aug. 10, 2024, 6:47 p.m.

App Security Score:

44/100 (MEDIUM RISK)

Grade:

B

Trackers Detection:

1/432

FINDINGS SEVERITY

∯ HIGH	▲ MEDIUM	i INFO	✓ SECURE	Q HOTSPOT
	26	1	0	1



File Name: 5009_5.3.3_3877.apk

Size: 13.47MB

MD5: 08bcb02717c33ca8708a341ba22fe81b

SHA1: 659daa1d24812b9e9c964d1971c2321349ff2c1f

SHA256: 3baa6f60d355d8d9366996b12cd7fe15cb943448c801a699f41ac631f3bd775b

i APP INFORMATION

App Name: Sync Services **Package Name:** com.fp.backup

Main Activity: com.fp.EndUserAgreementActivity

Target SDK: 26 Min SDK: 15 Max SDK:

Android Version Name: 5.3.3
Android Version Code: 1



Activities: 7
Services: 11
Receivers: 7
Providers: 2

Exported Activities: 0 Exported Services: 8 Exported Receivers: 6 Exported Providers: 0

***** CERTIFICATE INFORMATION

Binary is signed v1 signature: True v2 signature: True v3 signature: True v4 signature: False

X.509 Subject: C=GB, ST=45v9z, L=l8kdy, O=vr2jn, OU=dpklm, CN=9t1fi

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2024-06-29 14:33:40+00:00 Valid To: 2079-04-02 14:33:40+00:00

Issuer: C=GB, ST=45v9z, L=l8kdy, O=vr2jn, OU=dpklm, CN=9t1fi

Serial Number: 0x79f2fac5 Hash Algorithm: sha256

md5: 2be09b2fc2f915afbb1fb1fa4da43533

sha1: 415bc0a0a87857d3378f334e44062722960f16d9

sha256: 6a4445cd472116796adbbe9b8de1a0d64b87f4ace46fcc33759e107f945dada7 sha512: a71a231972b7c69118519bafa42128f3d2828548612477b3e807806df8ec5eaa7929d93d843dd66cd082e957522e06235078a1d20820f239ee48709057e51e04 PublicKey Algorithm: rsa Bit Size: 2048

 $Fingerprint: bfc6868a5063df78d02089504737dad3fbc9d3a83426b1d50fef46979a846db3\\ Found 1 unique certificates$

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
android.permission.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.KILL_BACKGROUND_PROCESSES	normal	kill background processes	Allows an application to kill background processes of other applications, even if memory is not low.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
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_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_CALL_LOG	dangerous	allows writing to (but not reading) the user's call log.	Allows an application to write (but not read) the user's call log data.
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_SMS	dangerous	edit SMS or MMS	Allows application to write to SMS messages stored on your phone or SIM card. Malicious applications may delete your messages.
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.
com.android.browser.permission.READ_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.sec.android.provider.logsprovider.permission.READ_LOGS	unknown	Unknown permission	Unknown permission from android reference
com.sec.android.provider.logsprovider.permission.WRITE_LOGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_SYNC_SETTINGS	normal	write sync settings	Allows an application to modify the sync settings, such as whether sync is enabled for Contacts.
android.permission.READ_SYNC_SETTINGS	normal	read sync settings	Allows an application to read the sync settings, such as whether sync is enabled for Contacts.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
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.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.GET_PACKAGE_SIZE	normal	measure application storage space	Allows an application to find out the space used by any package.
android.permission.ACCESS_SUPERUSER	unknown	Unknown permission	Unknown permission from android reference
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.

PERMISSION	STATUS	INFO	DESCRIPTION
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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
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.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.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.fp.backup.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference

ক্ল APKID ANALYSIS

FILE	DETAILS	
	FINDINGS	DETAILS
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.BOARD check possible Build.SERIAL check network operator name check
	Compiler	unknown (please file detection issue!)



NO SCOPE SEVERITY DESCRIPTION	NO	SCOPE	SEVERITY	
-------------------------------	----	-------	----------	--

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE SEVERITY DESCRIPTI		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.

Q MANIFEST ANALYSIS

HIGH: 1 | WARNING: 16 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.0.3-4.0.4, [minSdk=15]	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	Service (com.fp.CoreService) 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.
3	Service (com.fp.spy_call.service.SpyService) 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.
4	Service (com.fp.WDService) 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.
5	Service (com.fp.capture.appscreenshot.ProjectionService) 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.
6	Broadcast Receiver (com.fp.receiver.CommonReceiver) 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.fp.callhandler.phonestate.OutgoingCallReceiver) 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
8	Service (com.fp.accessibilityservice.NMAccessibilityService) 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.
9	Broadcast Receiver (com.fp.receiver.AppDeviceAdminReceiver) 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.
10	Service (com.fp.google_push_notification_manager.MyFirebaseInstanceIDService) 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.
11	Broadcast Receiver (com.fp.google_push_notification_manager.FirebaseDataReceiver) 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.
12	Service (com.fp.capture.callrecorder.accessibility_use.VoIPCallRecordingStateNotifier) 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.
13	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
14	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
15	Service (com.google.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.
16	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

NO	ISSUE	SEVERITY	DESCRIPTION
17	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: 2 | WARNING: 7 | INFO: 1 | SECURE: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/fp/addressbookmanager/c/b.java com/fp/datadeliverymanager/b/a/c.java com/fp/eventrepository/a/a.java com/fp/eventrepository/a/ac.java com/fp/eventrepository/a/af.java com/fp/eventrepository/a/ag.java com/fp/eventrepository/a/an.java com/fp/eventrepository/a/e.java com/fp/eventrepository/a/e.java com/fp/eventrepository/a/f.java com/fp/eventrepository/a/g.java com/fp/eventrepository/a/h.java com/fp/eventrepository/a/h.java com/fp/eventrepository/a/p.java com/fp/eventrepository/a/p.java com/fp/eventrepository/b/b.java com/fp/hoenix/prot/b/b.java com/fp/phoenix/prot/c.java com/fp/y/a.java
2	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	a_vcard/android/content/ContentValues.java a_vcard/android/syncml/pim/VDataBuilder.java a_vcard/android/syncml/pim/vcard/ContactStruc t.java a_vcard/android/syncml/pim/vcard/VCardParser _V21.java a_vcard/android/syncml/pim/vcard/VCardParser _V30.java com/fp/a/c.java com/fp/a/d.java com/fp/a/d.java com/fp/logger/b.java com/fp/logger/d.java com/fp/p/c.java com/fp/c.java defpackage/ReadExample.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/codebutler/android_websockets/a.java
4	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/fp/ap/b/d.java com/fp/appengine/a/ag.java com/fp/aq/a/a.java com/fp/io/e.java
5	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/fp/u/a.java
6	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	net/lingala/zip4j/crypto/AESEncrpyter.java net/lingala/zip4j/crypto/StandardEncrypter.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	a_vcard/android/provider/Contacts.java
8	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/fp/logger/b.java
9	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/fp/l/a.java
10	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/fp/ab/b.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/libflsonyconfig.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	armeabi-v7a/libflsamsungconfig.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
3	armeabi-v7a/libflmotoconfig.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	armeabi-v7a/libmp3lame.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/libflhtcconfig.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	armeabi-v7a/libflasusconfig.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	armeabi-v7a/libfllgconfig.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	arm64-v8a/libflsonyconfig.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.
9	arm64-v8a/libflsamsungconfig.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	arm64-v8a/libflmotoconfig.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.
11	arm64-v8a/libmp3lame.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
12	arm64-v8a/libflhtcconfig.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
13	arm64-v8a/libflasusconfig.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.
14	arm64-v8a/libfllgconfig.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.
15	armeabi-v7a/libflsonyconfig.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
16	armeabi-v7a/libflsamsungconfig.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.
17	armeabi-v7a/libflmotoconfig.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.
18	armeabi-v7a/libmp3lame.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	armeabi-v7a/libflhtcconfig.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.
20	armeabi-v7a/libflasusconfig.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.
21	armeabi-v7a/libfllgconfig.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	arm64-v8a/libflsonyconfig.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.
23	arm64-v8a/libflsamsungconfig.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.
24	arm64-v8a/libflmotoconfig.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
25	arm64-v8a/libmp3lame.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.
26	arm64-v8a/libflhtcconfig.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.
27	arm64-v8a/libflasusconfig.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
28	arm64-v8a/libfllgconfig.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	19/24	android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_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_PHONE_STATE, android.permission.READ_SMS, android.permission.RECEIVE_SMS, android.permission.SEND_SMS, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.RECORD_AUDIO, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	14/45	android.permission.AUTHENTICATE_ACCOUNTS, android.permission.CALL_PHONE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.PROCESS_OUTGOING_CALLS, android.permission.WRITE_CONTACTS, android.permission.WRITE_SMS, com.google.android.c2dm.permission.RECEIVE, android.permission.READ_CALENDAR, android.permission.ACCESS_SUPERUSER, android.permission.BLUETOOTH, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.REQUEST_INSTALL_PACKAGES, android.permission.PACKAGE_USAGE_STATS, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

DOMAIN COUNTRY/REGION

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
maps.google.com	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.google.com	ok	IP: 142.251.39.4 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.mp3dev.org	ok	IP: 142.251.39.51 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
fppush-7a95f.firebaseio.com	ok	IP: 34.120.206.254 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map

DOMAIN	STATUS	GEOLOCATION
mandrillapp.com	ok	IP: 44.240.4.87 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://fppush-7a95f.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

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

₽ HARDCODED SECRETS

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AlzaSyA62LG44BEN-ZZQ3a1zNTo0wRzvpvviJ9Q"
"google_api_key" : "AlzaSyA62LG44BEN-ZZQ3a1zNTo0wRzvpvviJ9Q"
"firebase_database_url" : "https://fppush-7a95f.firebaseio.com"
Hy4wDUI8WylalwYeN0Q3N31dJyceS3tMEDd8WSprI1AoMgpbPRoyO1gp
PQYUOBkGHxg2AXM7ChlbB1llDAg7CV8cMQYdAgsy

POSSIBLE SECRETS

258EAFA5-E914-47DA-95CA-C5AB0DC85B11

aHR0cHM6Ly93d3cuZmxleGlzcHkuY29tL2VuL2luc3RhbGxhdGlvbi1ldWxhLmh0bQ==

CwlvaRU8GDsTNX0YMD0gCmdVGQ4LA1MPEUNfETEOSVU=

HQoXKhAlAwsfBlo4CgETH1YKDRYwEF4BcRFcDA==

01360240043788015936020505

∷ SCAN LOGS

Timestamp	Event	Error
2024-08-10 18:47:36	Generating Hashes	ОК
2024-08-10 18:47:36	Extracting APK	ОК
2024-08-10 18:47:36	Unzipping	ОК
2024-08-10 18:47:37	Getting Hardcoded Certificates/Keystores	ОК
2024-08-10 18:47:38	Parsing AndroidManifest.xml	ОК
2024-08-10 18:47:38	Parsing APK with androguard	ОК
2024-08-10 18:47:38	Extracting Manifest Data	ОК
2024-08-10 18:47:38	Performing Static Analysis on: Sync Services (com.fp.backup)	OK

2024-08-10 18:47:38	Fetching Details from Play Store: com.fp.backup	ОК
2024-08-10 18:47:39	Manifest Analysis Started	ОК
2024-08-10 18:47:39	Checking for Malware Permissions	ОК
2024-08-10 18:47:39	Fetching icon path	ОК
2024-08-10 18:47:39	Library Binary Analysis Started	ОК
2024-08-10 18:47:39	Analyzing lib/armeabi-v7a/libflsonyconfig.so	ОК
2024-08-10 18:47:39	Analyzing lib/armeabi-v7a/libflsamsungconfig.so	ОК
2024-08-10 18:47:39	Analyzing lib/armeabi-v7a/libflmotoconfig.so	ок
2024-08-10 18:47:39	Analyzing lib/armeabi-v7a/libmp3lame.so	ОК
2024-08-10 18:47:39	Analyzing lib/armeabi-v7a/libflhtcconfig.so	ок
2024-08-10 18:47:39	Analyzing lib/armeabi-v7a/libflasusconfig.so	ок
2024-08-10 18:47:40	Analyzing lib/armeabi-v7a/libfllgconfig.so	ОК
2024-08-10 18:47:40	Analyzing lib/arm64-v8a/libflsonyconfig.so	ОК
2024-08-10 18:47:40	Analyzing lib/arm64-v8a/libflsamsungconfig.so	OK
2024-08-10 18:47:40	Analyzing lib/arm64-v8a/libflmotoconfig.so	OK

2024-08-10 18:47:40	Analyzing lib/arm64-v8a/libmp3lame.so	ОК
2024-08-10 18:47:40	Analyzing lib/arm64-v8a/libflhtcconfig.so	ОК
2024-08-10 18:47:40	Analyzing lib/arm64-v8a/libflasusconfig.so	ОК
2024-08-10 18:47:40	Analyzing lib/arm64-v8a/libfllgconfig.so	ОК
2024-08-10 18:47:40	Analyzing apktool_out/lib/armeabi-v7a/libflsonyconfig.so	ОК
2024-08-10 18:47:40	Analyzing apktool_out/lib/armeabi-v7a/libflsamsungconfig.so	ОК
2024-08-10 18:47:40	Analyzing apktool_out/lib/armeabi-v7a/libflmotoconfig.so	ОК
2024-08-10 18:47:40	Analyzing apktool_out/lib/armeabi-v7a/libmp3lame.so	ОК
2024-08-10 18:47:41	Analyzing apktool_out/lib/armeabi-v7a/libflhtcconfig.so	ОК
2024-08-10 18:47:41	Analyzing apktool_out/lib/armeabi-v7a/libflasusconfig.so	ОК
2024-08-10 18:47:41	Analyzing apktool_out/lib/armeabi-v7a/libfllgconfig.so	ОК
2024-08-10 18:47:41	Analyzing apktool_out/lib/arm64-v8a/libflsonyconfig.so	ОК
2024-08-10 18:47:41	Analyzing apktool_out/lib/arm64-v8a/libflsamsungconfig.so	ОК
2024-08-10 18:47:41	Analyzing apktool_out/lib/arm64-v8a/libflmotoconfig.so	ОК
2024-08-10 18:47:41	Analyzing apktool_out/lib/arm64-v8a/libmp3lame.so	ОК

2024-08-10 18:47:41	Analyzing apktool_out/lib/arm64-v8a/libflhtcconfig.so	ОК
2024-08-10 18:47:41	Analyzing apktool_out/lib/arm64-v8a/libflasusconfig.so	ОК
2024-08-10 18:47:41	Analyzing apktool_out/lib/arm64-v8a/libfilgconfig.so	ОК
2024-08-10 18:47:41	Reading Code Signing Certificate	ОК
2024-08-10 18:47:42	Running APKiD 2.1.5	ОК
2024-08-10 18:47:44	Detecting Trackers	OK
2024-08-10 18:47:44	Decompiling APK to Java with jadx	ОК
2024-08-10 18:47:54	Converting DEX to Smali	OK
2024-08-10 18:47:54	Code Analysis Started on - java_source	ОК
2024-08-10 18:47:59	Android SAST Completed	OK
2024-08-10 18:47:59	Android API Analysis Started	ОК
2024-08-10 18:48:02	Android Permission Mapping Started	ОК
2024-08-10 18:48:35	Android Permission Mapping Completed	ОК
2024-08-10 18:48:36	Finished Code Analysis, Email and URL Extraction	ОК
2024-08-10 18:48:36	Extracting String data from APK	OK

2024-08-10 18:48:36	Extracting String data from SO	ОК
2024-08-10 18:48:36	Extracting String data from Code	ОК
2024-08-10 18:48:36	Extracting String values and entropies from Code	ОК
2024-08-10 18:48:38	Performing Malware check on extracted domains	ОК
2024-08-10 18:48:40	Saving to Database	ОК

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.

© 2024 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.