ANDROID STATIC ANALYSIS REPORT

File Name:	com-wondershare-famisafe-9669-68317696-16629e1060a1c92c71039b354d5468ee.apk
Package Name:	com.wondershare.famisafe
Scan Date:	Oct. 27, 2025, 6:29 a.m.
App Security Score:	42/100 (MEDIUM RISK)
Grade:	

B

Trackers Detection: 8/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	21	0	0	1

FILE INFORMATION

File Name: com-wondershare-famisafe-9669-68317696-16629e1060a1c92c71039b354d5468ee.apk
Size: 94.85MB
MD5: 16629e1060a1c92c71039b354d5468ee
SHA1: 0774930daaa5c1ffd8c0ff3017b39da389b57ac6
SHA256: eb45e96166cea33b1700fdb9a4153a6212b3ce0a7e2903bcd00e098ef8a3326b

APP INFORMATION

App Name: FamiSafe
Package Name: com.wondershare.famisafe
Main Activity: com.wondershare.famisafe.CheckRoleSplashActivity
Target SDK: 33
Min SDK: 19
Max SDK:
Android Version Name: 7.2.5.9669
Android Version Code: 9669

APP COMPONENTS

Activities: 124
Services: 15
Receivers: 11
Providers: 6
Exported Activities: 3
Exported Services: 3
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=CHINA, ST=GD, L=SZ, O=com.wondershare, OU=com.wondershare, CN=com.wondershare
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-05-08 10:26:39+00:00
Valid To: 2043-05-02 10:26:39+00:00
Issuer: C=CHINA, ST=GD, L=SZ, O=com.wondershare, OU=com.wondershare, CN=com.wondershare
Serial Number: 0x1ff7cbe
Hash Algorithm: sha256
md5: c934e6c4883c63a2b8d791d4874d2328
sha1: 61b90229f79f730043d06fee46bb8fd9e3a0e70b
sha256: da624a72d8a9f54729710d79d8d98bfaa3beebfcebca352e70405e3756ba835e
sha512: da38e7c75c1cc74371713d91873b19238647ca6ad72dd0b9250e9da4a8b61084de0b51c14f6ee0cc8ce87793443009483fb1b3f67effa9d3073396797ab57b79
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c11a2b379a67eddab8cd1e1d2dddabfbf67c6b73051564ef8778e5f67e922165
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.

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_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	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.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.android.alarm.permission.SET_ALARM	unknown	Unknown permission	Unknown permission from android reference
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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
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.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
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.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
com.wondershare.famisafe.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.

APKID ANALYSIS

FILE	DETAILS
	FINDINGS | DETAILS

classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check SIM operator check network operator name check ro.kernel.qemu check possible VM check
	Obfuscator	unreadable field names unreadable method names
	Compiler	r8 without marker (suspicious)

classes2.dex

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.TAGS check
Compiler	r8 without marker (suspicious)

classes3.dex

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check
Compiler	r8 without marker (suspicious)

classes4.dex	

FINDINGS	DETAILS
Anti-VM Code	Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check
Compiler	r8 without marker (suspicious)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.wondershare.famisafe.CheckRoleSplashActivity	Schemes: http://, https://, famisafe://, pchjzh://, Hosts: famisafe.page.link, fb, allapp.link, Path Prefixes: /deeplink1,
com.sensorsdata.analytics.android.sdk.dialog.SchemeActivity	Schemes: sa1951ae34://,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.wondershare.famisafe,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 3 | WARNING: 19 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.4-4.4.4, [minSdk=19]	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.
			An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity

3	Launch Mode of activity (com.wondershare.famisafe.share.account.RegisterAct) is not standard.	warning	and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
4	App Link assetlinks.json file not found [android:name=com.wondershare.famisafe.CheckRoleSplashActivity] [android:host=http://famisafe.page.link]	high	App Link asset verification URL (http://famisafe.page.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
5	Launch Mode of activity (com.sensorsdata.analytics.android.sdk.dialog.SchemeActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
6	Activity (com.sensorsdata.analytics.android.sdk.dialog.SchemeActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Service (com.wondershare.famisafe.parent.ParentNotifyService) 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.
8	Launch Mode of activity (com.wondershare.famisafe.parent.guide.AuthorizeWaitActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
			An Activity should not be having the launch mode attribute

9	Launch Mode of activity (com.wondershare.famisafe.parent.reconnect.ReconnectActivity) is not standard.	warning	set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
10	Launch Mode of activity (com.wondershare.famisafe.parent.home.MainParentActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
11	Launch Mode of activity (com.wondershare.famisafe.parent.feature.AllFeatureActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
12	Broadcast Receiver (com.wondershare.famisafe.parent.reconnect.NetworkReconnectReceiver) is not Protected. [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.
13	Broadcast Receiver (com.appsflyer.SingleInstallBroadcastReceiver) is not Protected. [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.
14	Activity (com.wondershare.famsiafe.billing.PayActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
15	Launch Mode of activity (com.wondershare.famisafe.share.CommonWebActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

16	Launch Mode of activity (com.wondershare.famisafe.share.account.LoginHomeActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
17	Launch Mode of activity (com.wondershare.famisafe.share.account.LoginAct) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
18	Launch Mode of activity (com.wondershare.famisafe.share.account.RoleActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
19	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
20	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is		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,

21	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	the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
22	Service (com.evernote.android.job.gcm.PlatformGcmService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_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.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
		True info The binary has NX bit set. This	True info This binary has a stack canary value	Full RELRO info This shared object has full RELRO	None info The binary does not	None info The binary does not have	False warning The binary does not have any fortified functions. Fortified	False warning Symbols are available.

1	x86/libRSSupport.so	marks a memory page non-executable making attacker injected shellcode non-executable.	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.	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.	have run-time search path or RPATH set.	RUNPATH set.	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.	
2	x86/libpl_droidsonroids_gif.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.
		True	True	Full RELRO	None	None	False	False

3	x86/librsjni_androidx.so	info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	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.	info The binary does not have run-time search path or RPATH set.	info The binary does not have RUNPATH set.	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.	warning Symbols are available.
4	x86/librsjni.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	mips/libpl_droidsonroids_gif.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/libRSSupport.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	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	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.

			integrity of the canary before function return.	both) is marked as read-only.				
7	armeabi-v7a/libpl_droidsonroids_gif.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	armeabi-v7a/librsjni_androidx.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-	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	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,	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.	False warning Symbols are available.

		executable.	detection of overflows by verifying the integrity of the canary before function return.	the entire GOT (.got and .got.plt both) is marked as read-only.			This check is not applicable for Dart/Flutter libraries.	
9	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.	True info The binary has the following fortified functions: ['__vsprintf_chk']	False warning Symbols are available.
		True info The binary has NX bit set. This marks a memory page non-executable making attacker	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	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten	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	False warning Symbols are available.

10	armeabi-v7a/librsjni.so	injected shellcode non-executable.	the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.			compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	
11	mips64/libpl_droidsonroids_gif.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.
		True info The binary has NX bit set. This marks a	True info This binary has a stack canary value added to the	Full RELRO info This shared object has full RELRO enabled.	None info The binary does not have	None info The binary does not have RUNPATH	True info The binary has the following fortified functions: ['__vsnprintf_chk',	False warning Symbols are available.

12	x86_64/libRSSupport.so	memory page non-executable making attacker injected shellcode non-executable.	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.	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.	run-time search path or RPATH set.	set.	'__strlen_chk', '__fgets_chk', '__vsprintf_chk', '__strncat_chk', '__strrchr_chk', '__memcpy_chk']	
13	x86_64/libpl_droidsonroids_gif.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.
		True info The binary	True info This binary	Full RELRO info This shared	None info The	None info The binary	False warning The binary does not	False warning Symbols are

14	x86_64/librsjni_androidx.so	has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	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.	binary does not have run-time search path or RPATH set.	does not have RUNPATH set.	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.	available.
15	x86_64/librsjni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

16	arm64-v8a/libRSSupport.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__fgets_chk', '__vsprintf_chk', '__strncat_chk', '__strrchr_chk', '__memcpy_chk']	False warning Symbols are available.
17	arm64-v8a/libpl_droidsonroids_gif.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	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	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.

			function return.	read-only.				
18	arm64-v8a/librsjni_androidx.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.
19	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	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	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsprintf_chk', '__strcat_chk']	False warning Symbols are available.

			verifying the integrity of the canary before function return.	and .got.plt both) is marked as read-only.				
20	arm64-v8a/librsjni.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/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode	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	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries.	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	False warning Symbols are available.

		non-executable.	allows detection of overflows by verifying the integrity of the canary before function return.	In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.			to fortify functions. This check is not applicable for Dart/Flutter libraries.	
22	x86/libRSSupport.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.
		True info The binary has NX bit set. This marks a memory page non-executable making	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be	None info The binary does not have run-time search path or RPATH	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,	False warning Symbols are available.

23	x86/libpl_droidsonroids_gif.so	attacker injected shellcode non-executable.	that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	set.		gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	
24	x86/librsjni_androidx.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.
		True info The binary has NX bit set. This marks a memory	True info This binary has a stack canary value added to the stack so that it	Full RELRO info This shared object has full RELRO enabled. RELRO	None info The binary does not have run-time	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow	False warning Symbols are available.

25	x86/librsjni.so	page non-executable making attacker injected shellcode non-executable.	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.	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.	search path or RPATH set.		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.	
26	mips/libpl_droidsonroids_gif.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.
		True info The binary has NX bit	True info This binary has a stack	Full RELRO info This shared object has	None info The binary	None info The binary does not	False warning The binary does not have any fortified	False warning Symbols are available.

27	armeabi-v7a/libRSSupport.so	set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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 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.	does not have run-time search path or RPATH set.	have RUNPATH set.	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.	
28	armeabi-v7a/libpl_droidsonroids_gif.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.
		True	True	Full RELRO	None	None	False	False

29	armeabi-v7a/librsjni_androidx.so	info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	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.	info The binary does not have run-time search path or RPATH set.	info The binary does not have RUNPATH set.	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.	warning Symbols are available.
30	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	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsprintf_chk']	False warning Symbols are available.

			return.					
31	armeabi-v7a/librsjni.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.
32	mips64/libpl_droidsonroids_gif.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	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	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.

			integrity of the canary before function return.	both) is marked as read-only.				
33	x86_64/libRSSupport.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__fgets_chk', '__vsprintf_chk', '__strncat_chk', '__strrchr_chk', '__memcpy_chk']	False warning Symbols are available.
34	x86_64/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-	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	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,	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.	False warning Symbols are available.

		executable.	detection of overflows by verifying the integrity of the canary before function return.	the entire GOT (.got and .got.plt both) is marked as read-only.			This check is not applicable for Dart/Flutter libraries.	
35	x86_64/librsjni_androidx.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.
36	x86_64/librsjni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker	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	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten	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	False warning Symbols are available.

		injected shellcode non-executable.	the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.			compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	
37	arm64-v8a/libRSSupport.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__fgets_chk', '__vsprintf_chk', '__strncat_chk', '__strrchr_chk', '__memcpy_chk']	False warning Symbols are available.
		True info The binary has NX bit set. This marks a memory page non-	True info This binary has a stack canary value added to the stack so that it will be	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that	None info The binary does not have run-time search	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	False warning Symbols are available.

38	arm64-v8a/libpl_droidsonroids_gif.so	executable making attacker injected shellcode non-executable.	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.	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.	path or RPATH set.		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.	
39	arm64-v8a/librsjni_androidx.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.
		True info The binary has NX bit set. This	True info This binary has a stack canary value	Full RELRO info This shared object has full RELRO	None info The binary does not	None info The binary does not have	True info The binary has the following fortified functions:	False warning Symbols are available.

40	arm64-v8a/libmp3lame.so	marks a memory page non-executable making attacker injected shellcode non-executable.	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.	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.	have run-time search path or RPATH set.	RUNPATH set.	['__vsprintf_chk', '__strcat_chk']	
41	arm64-v8a/librsjni.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.
		True info	True info	Full RELRO info	None info	None info	False warning	False warning

42	armeabi/libpl_droidsonroids_gif.so	The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	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.	The binary does not have run-time search path or RPATH set.	The binary does not have RUNPATH set.	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.	Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/24	android.permission.VIBRATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.CAMERA, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED

Other Common Permissions	9/45	android.permission.ACCESS_BACKGROUND_LOCATION, com.google.android.gms.permission.ACTIVITY_RECOGNITION, android.permission.READ_CALENDAR, android.permission.BLUETOOTH, android.permission.FLASHLIGHT, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID, android.permission.CHANGE_WIFI_STATE

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
lame.sf.net	ok	**IP:** 104.18.20.237 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
famisafe-b6807.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

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://famisafe-b6807.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

TRACKER	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sensors Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/248

HARDCODED SECRETS

POSSIBLE SECRETS
"authorization" : "Autorizzazione"
"lbPassword" : "パスワード"
"permission_white_doze_key" : "バッテリーの最適化を無視"
"pref_key_cbp14_title" : "Warnung"
"pref_key_cbp14_title" : "Avviso"
"account_tip_pwd_length" : "パスワードは6〜32文字の長さである必要があります。"
"lbPassword" : "Kennwort"
"pref_key_cbp15_default" : "true"
"enter_password" : "パスワード"
"pref_key_cbp14_title" : "アラート"
"sus_key_remove_tip" : "設定後、XXXは検出されなくなり、怪しい言葉ライブラリから削除されます。続行しますか？"
"pref_key_cbp6" : "pref_cbp6"
"lbPassword" : "Contraseña"
"lbPassword" : "Senha"
"pref_key_cbp9_default" : "true"

"reset_password" : "パスワードをリセットする"
"lbWrongNameOrPassword" : "メールまたはパスワードが間違っています"
"pref_key_cbp9_title" : "お子様からのリクエスト"
"enter_password" : "Senha"
"com_facebook_device_auth_instructions" : "facebook.com/deviceにアクセスして、上記のコードを入力してください。"
"pref_key_cbp12_title" : "Articles"
"enter_password" : "Password"
"com_facebook_device_auth_instructions" : "访问facebook.com/device并输入上方显示的验证码。"
"lbPassword" : "Password"
"pref_key_cbp14_default" : "true"
"pref_key_cbp6_title" : "お子様のデバイスを新たに接続する場合"
"pref_key_cbp13" : "pref_cbp13"
"pref_key_cbp14_title" : "Alerta"
"enter_your_password" : "パスワードを入力してください"
"pref_key_cbp12_title" : "リソース"
"firebase_database_url" : "https://famisafe-b6807.firebaseio.com"
"pref_key_cbp12_title" : "Beiträge"
"sus_key_remove_setting" : "Erinnerungseinstellungen"

"sus_key_remove_setting" : "Erinnerungseinstellungen"

"lbPassword" : "비밀번호"

"pref_key_cbp9" : "pref_cbp9"

"google_api_key" : "AIzaSyDXMlASBQ6sbSVZsvZn4N3JHRQpP2WURWU"

"pref_key_cbp15" : "pref_cbp15"

"authorization" : "Authorization"

"sus_key_remove_setting_tip" : "検出を停止するワードを選択してください"

"pref_key_cbp7" : "pref_cbp7"

"pref_key_cbp12" : "pref_cbp12"

"authorization" : "Autorisierung"

"enter_password" : "비밀번호"

"pref_key_cbp14_title" : "Alerte"

"com.google.firebase.crashlytics.mapping_file_id" : "a118ded53dfb4c70a3fd9f31f35a6528"

"pref_key_cbp6_default" : "false"

"forgetpassword" : "パスワードを忘れた"

"enter_password" : "Contraseña"

"lbforgetpassword" : "パスワードをお忘れですか？"

"pref_key_cbp7_title" : "不明な問題が発生した場合"

"google_crash_reporting_api_key" : "AIzaSyDXMlASBQ6sbSVZsvZn4N3JHRQpP2WURWU"
"pref_key_cbp13_default" : "true"
"sus_key_remove_setting" : "リマインダーの設定"
"uninstall_user" : "私の親のアカウント：%s"
"pref_key_cbp14_title" : "경보"
"pref_key_cbp14_title" : "Alert"
"sus_key_remove_success" : "成功！このワードの検出結果を受け取らなくなります。"
"authorization" : "Autorização"
"pref_key_cbp12_title" : "Artigos"
"pref_key_cbp12_default" : "true"
"pref_key_cbp12_title" : "Resource"
"pref_key_cbp12_title" : "Articoli"
"pref_key_cbp7_default" : "true"
"authorization" : "認可"
"pref_key_cbp12_title" : "기사"
"authorization" : "Autorisation"
"sus_key_remove_title" : "ワードの検出を停止"
"pref_key_cbp12_title" : "Artículos"

"pref_key_cbp12_title" : "Artículos"
"pref_key_cbp14" : "pref_cbp14"
"pref_key_cbp6_default" : "true"
"authorization" : "Autorización"

PLAYSTORE INFORMATION

Title: Parental Control App- FamiSafe

Score: 4.0740743 **Installs:** 5,000,000+ **Price:** 0 **Android Version Support:** **Category:** Parenting **Play Store URL:** com.wondershare.famisafe

Developer Details: Shenzhen Wondershare Software Co., Ltd., Shenzhen+Wondershare+Software+Co.,+Ltd., None, https://famisafe.wondershare.com/, famisafe@wondershare.com,

Release Date: Jul 13, 2018 **Privacy Policy:** Privacy link

Description:

FamiSafe – Parental Control App is designed for caring parents to control their children's screen time, track location, and monitor digital habits. This versatile app ensures your child's safety with reliable tools to manage app usage, block inappropriate content, and monitor calls and messages. The latest version includes upgraded sensitive content monitoring. We support monitoring of sensitive emojis. emojis can convey as much meaning as words, and this feature ensures that your child's online interactions are safe. How can FamiSafe – Parental Control App help protect your child? Monitor Online Activities – Want to know what your child does with their phone every day? Concerned they might visit dangerous content? FamiSafe can help you monitor their online activities, including how much time they spend on each app and which websites they visit, What videos do they watch on youtube and tiktok. Calls & Messages Monitoring - Stay informed by monitoring your child's calls and texts, with keyword detection to ensure their safety from potential dangers. Location Tracker – Worried when your child doesn't respond, or when they're not by your side? FamiSafe's highly accurate GPS location tracker can help you know where they are and their historical whereabouts. Screen Time Control – Concerned about your child becoming addicted to mobile phones? FamiSafe's screen time controller can help you customize screen time limits, such as less screen time on school days and more on weekends. Blocksite & App Blocker – FamiSafe – App Blocker helps guide your child to age-appropriate content by filtering inappropriate web pages and blocking adult apps, such as porn, dating apps, and certain gaming apps. Screen Viewer - Parents can remotely capture their children's screenshots to monitor and enforce appropriate phone usage. Remote screen capture is available for mobile devices, Windows and Mac. One-Way Audio – This newly released function allows you to listen to your child's surroundings, the location sound tracker feature now lets you know what's happening around your kids to ensure they stay safe. This function empowers parents to stay connected and informed. Panic Button – If your child feels threatened when they are alone, they can use the SOS button on FamiSafe Kids. You will receive an SOS alert with their accurate location information, so you can help them right away. Sensitive words & sexual picture detection - with FamiSafe Parental Control App you can easily detect sensitive content on your child's phone, including keywords & associated emojis (such as drugs, addiction, depression, suicide, etc.) and sensitive pictures across various platforms like WhatsApp, Facebook, Snapchat, Discord, YouTube, Instagram, Twitter, and other apps. Compared to a spy app, FamiSafe is more like a family link, allowing parents to understand their child better and help them develop good digital device usage habits. To start protecting your child 1.Download the Parental Control App – FamiSafe on your phone. 2.Download FamiSafe Kids on your child's phone. 3.Pair the devices with the code to monitor your child remotely. A paid parent account can bind more than 5 children's devices at the same time, and parents can be added for co-parenting. FamiSafe does not contain any advertisement. Why should you choose FamiSafe- Parental Control App? Recognized and trusted by many organizations and associations * Best Products for

Elementary Kids 2024 * National Parenting Product Awards Winner 2024 * Best Middle & High School Products 2024 * Best Family Health & Safety Products 2024 ---POLICIES & TERMS OF USE--- Privacy Policy: https://www.wondershare.com/privacy.html Terms of Use: https://famisafe.wondershare.com/terms-of-use.html Website: https://famisafe.wondershare.com/ Contact US: customer_service@wondershare.com

SCAN LOGS

Timestamp	Event	Error
2025-10-27 06:29:14	Generating Hashes	OK
2025-10-27 06:29:14	Extracting APK	OK
2025-10-27 06:29:14	Unzipping	OK
2025-10-27 06:29:16	Getting Hardcoded Certificates/Keystores	OK
2025-10-27 06:29:35	Parsing AndroidManifest.xml	OK
2025-10-27 06:29:35	Parsing APK with androguard	OK
2025-10-27 06:29:36	Extracting Manifest Data	OK
2025-10-27 06:29:37	Performing Static Analysis on: FamiSafe (com.wondershare.famisafe)	OK

2025-10-27 06:29:37	Fetching Details from Play Store: com.wondershare.famisafe	OK
2025-10-27 06:29:38	Manifest Analysis Started	OK
2025-10-27 06:29:40	Checking for Malware Permissions	OK
2025-10-27 06:29:41	Fetching icon path	OK
2025-10-27 06:29:41	Library Binary Analysis Started	OK
2025-10-27 06:29:41	Analyzing apktool_out/lib/x86/libRSSupport.so	OK
2025-10-27 06:29:43	Analyzing apktool_out/lib/x86/libpl_droidsonroids_gif.so	OK
2025-10-27 06:29:43	Analyzing apktool_out/lib/x86/librsjni_androidx.so	OK
2025-10-27 06:29:43	Analyzing apktool_out/lib/x86/librsjni.so	OK
2025-10-27 06:29:43	Analyzing apktool_out/lib/mips/libpl_droidsonroids_gif.so	OK
2025-10-27 06:29:44	Analyzing apktool_out/lib/armeabi-v7a/libRSSupport.so	OK
2025-10-27 06:29:46	Analyzing apktool_out/lib/armeabi-v7a/libpl_droidsonroids_gif.so	OK

2025-10-27 06:29:46	Analyzing apktool_out/lib/armeabi-v7a/librsjni_androidx.so	OK
2025-10-27 06:29:46	Analyzing apktool_out/lib/armeabi-v7a/libmp3lame.so	OK
2025-10-27 06:29:47	Analyzing apktool_out/lib/armeabi-v7a/librsjni.so	OK
2025-10-27 06:29:47	Analyzing apktool_out/lib/mips64/libpl_droidsonroids_gif.so	OK
2025-10-27 06:29:50	Analyzing apktool_out/lib/x86_64/libRSSupport.so	OK
2025-10-27 06:29:56	Analyzing apktool_out/lib/x86_64/libpl_droidsonroids_gif.so	OK
2025-10-27 06:29:56	Analyzing apktool_out/lib/x86_64/librsjni_androidx.so	OK
2025-10-27 06:29:56	Analyzing apktool_out/lib/x86_64/librsjni.so	OK
2025-10-27 06:29:56	Analyzing apktool_out/lib/arm64-v8a/libRSSupport.so	OK
2025-10-27 06:29:59	Analyzing apktool_out/lib/arm64-v8a/libpl_droidsonroids_gif.so	OK
2025-10-27 06:29:59	Analyzing apktool_out/lib/arm64-v8a/librsjni_androidx.so	OK

2025-10-27 06:29:59	Analyzing apktool_out/lib/arm64-v8a/libmp3lame.so	OK
2025-10-27 06:29:59	Analyzing apktool_out/lib/arm64-v8a/librsjni.so	OK
2025-10-27 06:29:59	Analyzing apktool_out/lib/armeabi/libpl_droidsonroids_gif.so	OK
2025-10-27 06:30:00	Analyzing lib/x86/libRSSupport.so	OK
2025-10-27 06:30:03	Analyzing lib/x86/libpl_droidsonroids_gif.so	OK
2025-10-27 06:30:03	Analyzing lib/x86/librsjni_androidx.so	OK
2025-10-27 06:30:03	Analyzing lib/x86/librsjni.so	OK
2025-10-27 06:30:03	Analyzing lib/mips/libpl_droidsonroids_gif.so	OK
2025-10-27 06:30:03	Analyzing lib/armeabi-v7a/libRSSupport.so	OK
2025-10-27 06:30:06	Analyzing lib/armeabi-v7a/libpl_droidsonroids_gif.so	OK
2025-10-27 06:30:07	Analyzing lib/armeabi-v7a/librsjni_androidx.so	OK

2025-10-27 06:30:07	Analyzing lib/armeabi-v7a/libmp3lame.so	OK
2025-10-27 06:30:07	Analyzing lib/armeabi-v7a/librsjni.so	OK
2025-10-27 06:30:07	Analyzing lib/mips64/libpl_droidsonroids_gif.so	OK
2025-10-27 06:30:13	Analyzing lib/x86_64/libRSSupport.so	OK
2025-10-27 06:30:16	Analyzing lib/x86_64/libpl_droidsonroids_gif.so	OK
2025-10-27 06:30:16	Analyzing lib/x86_64/librsjni_androidx.so	OK
2025-10-27 06:30:16	Analyzing lib/x86_64/librsjni.so	OK
2025-10-27 06:30:16	Analyzing lib/arm64-v8a/libRSSupport.so	OK
2025-10-27 06:30:21	Analyzing lib/arm64-v8a/libpl_droidsonroids_gif.so	OK
2025-10-27 06:30:21	Analyzing lib/arm64-v8a/librsjni_androidx.so	OK
2025-10-27 06:30:21	Analyzing lib/arm64-v8a/libmp3lame.so	OK
2025-10-27 06:30:22	Analyzing lib/arm64-v8a/librsjni.so	OK

2025-10-27 06:30:22	Analyzing lib/armeabi/libpl_droidsonroids_gif.so	OK
2025-10-27 06:30:22	Reading Code Signing Certificate	OK
2025-10-27 06:30:29	Running APKiD 2.1.5	OK
2025-10-27 06:30:48	Updating Trackers Database....	OK
2025-10-27 06:30:48	Detecting Trackers	OK
2025-10-27 06:31:04	Decompiling APK to Java with jadx	OK
2025-10-27 06:31:04	Converting DEX to Smali	OK
2025-10-27 06:31:04	Code Analysis Started on - java_source	OK
2025-10-27 06:31:04	Android SAST Completed	OK
2025-10-27 06:31:04	Android API Analysis Started	OK
2025-10-27 06:31:09	Android Permission Mapping Started	OK

2025-10-27 06:31:09	Android Permission Mapping Completed	OK
2025-10-27 06:31:09	Finished Code Analysis, Email and URL Extraction	OK
2025-10-27 06:31:09	Extracting String data from APK	OK
2025-10-27 06:31:22	Extracting String data from SO	OK
2025-10-27 06:31:23	Extracting String data from Code	OK
2025-10-27 06:31:23	Extracting String values and entropies from Code	OK
2025-10-27 06:31:24	Performing Malware check on extracted domains	OK
2025-10-27 06:31:32	Saving to Database	OK

© 2025 | Android Static Analysis.