MOBSF

ANDROID STATIC ANALYSIS REPORT

Internet Service (14.6)

File Name:	iKeyMonitor-Android.apk
Package Name:	com.sec.android.internet.im.service.im20210815
Scan Date:	Aug. 10, 2024, 6:51 p.m.

App Security Score: 44/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
6	24	3	2	1

FILE INFORMATION

File Name: iKeyMonitor-Android.apk
Size: 14.32MB

MD5: d27a02b55549c9ab5c9c579608713cbc
SHA1: 180d8e9a243285c6db8b402f9bfe37cf98a7c45f
SHA256: 4de86cd9d6a7a7ed00d552c706ea3ac7f2507df81cf1b59388a9aa7b8af94412

APP INFORMATION

App Name: Internet Service
Package Name: com.sec.android.internet.im.service.im20210815
Main Activity: com.as.monitoringapp.Activity.SplashScreen
Target SDK: 29
Min SDK: 21
Max SDK:
Android Version Name: 14.6
Android Version Code: 322

APP COMPONENTS

Activities: 34
Services: 22
Receivers: 16
Providers: 3
Exported Activities: 1
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=01, ST=1, L=CA, O=CA, OU=UA, CN=CA
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-08-13 02:48:42+00:00
Valid To: 2046-08-07 02:48:42+00:00
Issuer: C=01, ST=1, L=CA, O=CA, OU=UA, CN=CA
Serial Number: 0x57ceaa3d
Hash Algorithm: sha256
md5: 847ad7be72a8a166fee2cc46078dfabb
sha1: 9284cb43b87e9f9c77da509f1672e884bd6ca876
sha256: 3cdc9034cce775d12b1998322a3fca2c7384e197290ee851c205a91786a61e43
sha512: 320765984951d401bbd2918a7955bb706589cf120d03dcd4b49a44ed6c3af793cce63d664e3db5889eba7540e4323e96ac224e5c7291634c956e1dc7ad1bc308
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 680ff8d866cb230b91a3ad7fc1cd1e94cc930779c4711c3ef249150a22098142
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
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_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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
android.permission.REBOOT	SignatureOrSystem	force phone reboot	Allows the application to force the phone to reboot.
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.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.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.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.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_LOGS	dangerous	read sensitive log data	Allows an application to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information.
android.permission.WRITE_LOGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_PRIVILEGED_PHONE_STATE	unknown	Unknown permission	Unknown permission from android reference
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.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
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
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_USER_DICTIONARY	dangerous	read user-defined dictionary	Allows an application to read any private words, names and phrases that the user may have stored in the user dictionary.
android.permission.WRITE_USER_DICTIONARY	normal	write to user-defined dictionary	Allows an application to write new words into the user dictionary.
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.INTERACT_ACROSS_USERS_FULL	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.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.BIND_ACCESSIBILITY_SERVICE	signature	required by AccessibilityServices for system binding.	Must be required by an AccessibilityService, to ensure that only the system can bind to it.
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
com.android.launcher.permission.INSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.UNINSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.READ_SETTINGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
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.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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.RESTART_PACKAGES	normal	kill background processes	Allows an application to kill background processes of other applications, even if memory is not low.
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
android.permission.CAPTURE_AUDIO_OUTPUT	SignatureOrSystem	allows capturing of audio output.	Allows an application to capture audio output.
android.permission.POST_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.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.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.as.monitoringapp.Activity.TrialPage	Schemes: smartkey://,

NETWORK SECURITY

HIGH: **3** | WARNING: **1** | INFO: **0** | SECURE: **0**

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.
3	*	high	Base config is configured to trust user installed certificates.

NO	SCOPE	SEVERITY	DESCRIPTION
4	emcpanel.com awsapi.io	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

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: 1 | WARNING: 11 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Activity (com.as.monitoringapp.Activity.TrialPage) 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.
4	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
5	High Intent Priority (2147483605) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
6	High Intent Priority (2147483605) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
7	High Intent Priority (2147483645) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

NO	ISSUE	SEVERITY	DESCRIPTION
8	High Intent Priority (2147483644) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
9	High Intent Priority (2147483643) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
10	High Intent Priority (2147483642) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
11	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
12	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
13	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: **9** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/a.java a1/h.java b0/f.java b0/q.java b1/i.java b4/f.java c0/b.java c0/c.java c0/d.java c2/e0.java c2/f.java c2/j.java c2/j0.java c2/k.java c2/v.java c2/z.java com/as/monitoringapp/Activity/ChangePassword.java com/as/monitoringapp/Activity/ChangePin.java com/as/monitoringapp/Activity/FloatActivity.java com/as/monitoringapp/Activity/Home.java com/as/monitoringapp/Activity/ImageGridActivity.java com/as/monitoringapp/Activity/Logging.java com/as/monitoringapp/Activity/LoginPage.java com/as/monitoringapp/Activity/ResetPasswordActivity.java com/as/monitoringapp/Activity/SettingsActivityNew.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/as/monitoringapp/Activity/SplashScreen.java com/as/monitoringapp/Activity/TrialPage.java com/as/monitoringapp/Activity/Wizard/Wizard0_Over_Protect_Activity.java com/as/monitoringapp/Activity/Wizard/Wizard1_Battery_Opt_Saver_Activity.java com/as/monitoringapp/Activity/Wizard/Wizard2_UsageAccess_Accessibility.java com/as/monitoringapp/Activity/Wizard/Wizard3_NoRoot_ScreenShot_Activity.java com/as/monitoringapp/Activity/Wizard/Wizard4_StatusBar_HomeScreenIcon_Activity.java com/as/monitoringapp/Activity/Wizard/Wizard5_Settings_State_Activity_v3.java com/as/monitoringapp/Activity/Wizard/Wizard6_Completed_Activity.java com/as/monitoringapp/Activity/Wizard/Wizard_Agreement_Web5Activity.java com/as/monitoringapp/Activity/Wizard/Wizard_Agreement_WebActivity.java com/as/monitoringapp/Activity/Wizard/Wizard_StatusBar_HomeSc_Activity.java com/as/monitoringapp/Activity/Wizard/web_guide_expand_info/Singl_expand_list_Activity.java com/as/monitoringapp/Activity/floating_wizard_view/BannerView_W.java com/as/monitoringapp/Activity/floating_wizard_view/FloatingBall_Service.java com/as/monitoringapp/Activity/floating_wizard_view/FloatingWnd_Service.java com/as/monitoringapp/Activity/timelimit/AppLimitService.java com/as/monitoringapp/Activity/timelimit/SettingGuide.java com/as/monitoringapp/Camera/Camera2Service.java com/as/monitoringapp/logging/AppGuardDialogService.java com/as/monitoringapp/logging/AppGuardOverLayService.java com/as/monitoringapp/logging/BackService.java com/as/monitoringapp/logging/CallingRecordService.java com/as/monitoringapp/logging/CaptureService.java com/as/monitoringapp/logging/Get10ClpInfoReceiver.java com/as/monitoringapp/logging/GpsHandler.java com/as/monitoringapp/logging/LicenseReceiver.java com/as/monitoringapp/logging/MyApplication.java com/as/monitoringapp/logging/MyNotificationListenService.java com/as/monitoringapp/logging/StartupReceiver.java com/as/monitoringapp/logging/screenshot/ScreenAlertVideoSrv.java com/as/monitoringapp/root/PermissionsActivity.java com/bumptech/glide/b.java com/jssrc/resample/JSSRCResampler.java d/c.java d/e.java d/f.java d0/a.java d0/b.java d0/c.java d0/d.java d0/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	d0/h.java d0/j.java d0/j.java d0/k.java d0/l.java d0/m.java e2/e.java e2/i0.java e2/z.java e4/n.java e8/i.java f1/a.java f2/a.java f2/a1.java f2/c.java f2/j0.java f2/m0.java f2/n0.java f2/o0.java f2/q0.java f2/s.java f2/u.java f2/w0.java f8/a.java g/a.java g/b.java g0/d.java g0/e.java g1/d.java g1/h.java g1/i.java g1/j.java g1/k.java g1/n.java g1/p.java g7/e.java h/c.java h/d.java h1/d.java h1/f.java h1/i.java h2/b.java i0/b.java i0/j.java i0/l.java i2/f.java i2/n.java j/a.java j/g.java j0/c.java j0/e.java j1/a.java k0/h.java k0/i.java k0/k.java k0/q.java k0/z.java k1/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				k1/c.java k1/e.java k1/g.java k1/i.java k1/j.java k3/d.java l0/i.java l0/k.java l2/b.java l3/b.java m0/e.java m0/i.java n/f.java n/g.java n/h.java n/i.java n0/a.java n3/g.java net/sqlcipher/AbstractCursor.java net/sqlcipher/BulkCursorToCursorAdaptor.java net/sqlcipher/DatabaseUtils.java net/sqlcipher/DefaultDatabaseErrorHandler.java net/sqlcipher/database/SQLiteCompiledSql.java net/sqlcipher/database/SQLiteContentHelper.java net/sqlcipher/database/SQLiteCursor.java net/sqlcipher/database/SQLiteDatabase.java net/sqlcipher/database/SQLiteDebug.java net/sqlcipher/database/SQLiteOpenHelper.java net/sqlcipher/database/SQLiteProgram.java net/sqlcipher/database/SQLiteQuery.java net/sqlcipher/database/SQLiteQueryBuilder.java net/sqlcipher/database/SqliteWrapper.java o/b.java o/c.java o0/c.java o0/d.java o0/f.java o0/s.java o0/t.java o1/k.java p/a.java p2/q.java q0/l.java r/a.java r/a0.java r/b.java r/e.java r/i.java r/j.java r/k.java r/l.java r/n.java r/o.java r/w.java r/x.java r/y.java r/z.java r0/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				r0/e.java r0/g0.java r0/j0.java r0/m.java r0/t.java r0/u.java r0/y.java r1/a.java s/a.java s/b.java s/f.java t7/a.java u/b.java u/c.java u/d.java u/f.java u/g.java u/h.java u/i.java u/j.java u/k.java u/n.java u/s.java v/a.java v/c.java v/d.java v/e.java v/f.java v/g.java v/h.java v/i.java v/j.java v/k.java v/l.java v/m.java v/n.java v/o.java v/p.java v/q.java v/r.java v/s.java v/t.java v0/a.java v0/d.java v0/j.java v2/a.java v3/e.java v6/b.java v7/b.java w/a.java w/c.java w/e.java w/f.java w/h.java w5/a.java w5/e.java w5/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				w5/g.java w6/b.java x/c.java x/j.java x0/e.java x0/f.java x0/k.java x0/l.java x0/n.java x0/o.java x4/b.java y0/d.java y2/h.java y3/g.java y3/o.java y4/c.java z1/a.java z1/d.java
2	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	c0/c.java d0/a.java d0/b.java d0/c.java d0/d.java d0/g.java d0/h.java d0/l.java d0/m.java k1/c.java r/z.java v1/m0.java v1/t0.java
3	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	org/acra/collector/SharedPreferencesCollector.java s7/c.java x7/a.java
4	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	f8/a.java j7/d.java j7/h.java u/l.java w6/z.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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/as/monitoringapp/Activity/TrialPage.java com/as/monitoringapp/logging/screenshot/ScreenAlertVideoSrv.java g1/i.java h1/i.java j/c.java j/g.java k1/i.java org/acra/file/Directory.java r/y.java r5/e.java u/f.java u/k.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	f7/f.java f7/g.java f7/l.java f7/m.java t7/a.java
7	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/as/monitoringapp/logging/iKClipboardService.java
8	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	x4/c.java
9	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/as/monitoringapp/Activity/FloatActivity.java d/c.java d0/a.java g4/e.java h0/g.java k0/d.java k0/p.java k0/x.java u/s.java
10	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/as/monitoringapp/Activity/SettingsActivityNew.java r/k.java
11	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	r/i.java r/z.java
12	Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.	warning	CWE: CWE-200: Information Exposure OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/as/monitoringapp/Activity/ClientShowLogs.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
13	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	r/p.java
14	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	r/i.java
15	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	e4/h.java
16	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	x4/b.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libresrtmp.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: ['__strchr_chk', '__strncpy_chk', '__strrchr_chk', '__vsprintf_chk', '__FD_SET_chk', '__memcpy_chk', '__vsnprintf_chk']	False warning Symbols are available.
2	armeabi-v7a/libwebpModule.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__read_chk']	False warning Symbols are available.

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	armeabi-v7a/liblame.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/libvorbis-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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	armeabi-v7a/liblamemp3.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', '__vsprintf_chk']	False warning Symbols are available.
10	armeabi-v7a/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	armeabi-v7a/libogg.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
12	armeabi-v7a/libvorbis.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.
13	x86_64/libresrtmp.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: ['__strchr_chk', '__strncpy_chk', '__strrchr_chk', '__vsprintf_chk', '__FD_SET_chk', '__memcpy_chk', '__vsnprintf_chk']	False warning Symbols are available.
14	x86_64/libwebpModule.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	x86_64/librestreaming.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	x86_64/libshout-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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: ['__strcat_chk', '__strcpy_chk', '__strlen_chk']	False warning Symbols are available.
17	x86_64/liblamejni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
18	x86_64/libshout.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: ['__FD_SET_chk', '__vsnprintf_chk', '__strlen_chk', '__memcpy_chk', '__FD_ISSET_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	x86_64/liblame.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	x86_64/libvorbis-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	False warning Symbols are available.
21	x86_64/liblamemp3.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', '__vsprintf_chk']	False warning Symbols are available.
22	x86_64/libsqlcipher.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
23	x86_64/libogg.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	x86_64/libvorbis.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.
25	arm64-v8a/libresrtmp.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: ['__strchr_chk', '__strncpy_chk', '__strrchr_chk', '__vsprintf_chk', '__FD_SET_chk', '__memcpy_chk', '__vsnprintf_chk']	False warning Symbols are available.
26	arm64-v8a/libwebpModule.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
27	arm64-v8a/librestreaming.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.
28	arm64-v8a/libshout-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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: ['__strcat_chk', '__strcpy_chk', '__strlen_chk']	False warning Symbols are available.
29	arm64-v8a/liblamejni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
30	arm64-v8a/libshout.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: ['__FD_SET_chk', '__vsnprintf_chk', '__strlen_chk', '__memcpy_chk', '__FD_ISSET_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	arm64-v8a/liblame.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	arm64-v8a/libvorbis-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	False warning Symbols are available.
33	arm64-v8a/liblamemp3.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', '__vsprintf_chk']	False warning Symbols are available.
34	arm64-v8a/libsqlcipher.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
35	arm64-v8a/libogg.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	arm64-v8a/libvorbis.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.
37	armeabi-v7a/libresrtmp.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: ['__strchr_chk', '__strncpy_chk', '__strrchr_chk', '__vsprintf_chk', '__FD_SET_chk', '__memcpy_chk', '__vsnprintf_chk']	False warning Symbols are available.
38	armeabi-v7a/libwebpModule.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__read_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
39	armeabi-v7a/librestreaming.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.
40	armeabi-v7a/libshout-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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: ['__strcat_chk', '__strcpy_chk', '__strlen_chk']	False warning Symbols are available.
41	armeabi-v7a/liblamejni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
42	armeabi-v7a/libshout.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: ['__FD_SET_chk', '__vsnprintf_chk', '__strlen_chk', '__memcpy_chk', '__FD_ISSET_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
43	armeabi-v7a/liblame.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.
44	armeabi-v7a/libvorbis-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.
45	armeabi-v7a/liblamemp3.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', '__vsprintf_chk']	False warning Symbols are available.
46	armeabi-v7a/libsqlcipher.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
47	armeabi-v7a/libogg.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.
48	armeabi-v7a/libvorbis.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.
49	x86_64/libresrtmp.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: ['__strchr_chk', '__strncpy_chk', '__strrchr_chk', '__vsprintf_chk', '__FD_SET_chk', '__memcpy_chk', '__vsnprintf_chk']	False warning Symbols are available.
50	x86_64/libwebpModule.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
51	x86_64/librestreaming.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.
52	x86_64/libshout-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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: ['__strcat_chk', '__strcpy_chk', '__strlen_chk']	False warning Symbols are available.
53	x86_64/liblamejni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
54	x86_64/libshout.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: ['__FD_SET_chk', '__vsnprintf_chk', '__strlen_chk', '__memcpy_chk', '__FD_ISSET_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
55	x86_64/liblame.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.
56	x86_64/libvorbis-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	False warning Symbols are available.
57	x86_64/liblamemp3.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', '__vsprintf_chk']	False warning Symbols are available.
58	x86_64/libsqlcipher.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
59	x86_64/libogg.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.
60	x86_64/libvorbis.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.
61	arm64-v8a/libresrtmp.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: ['__strchr_chk', '__strncpy_chk', '__strrchr_chk', '__vsprintf_chk', '__FD_SET_chk', '__memcpy_chk', '__vsnprintf_chk']	False warning Symbols are available.
62	arm64-v8a/libwebpModule.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
63	arm64-v8a/librestreaming.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.
64	arm64-v8a/libshout-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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: ['__strcat_chk', '__strcpy_chk', '__strlen_chk']	False warning Symbols are available.
65	arm64-v8a/liblamejni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
66	arm64-v8a/libshout.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: ['__FD_SET_chk', '__vsnprintf_chk', '__strlen_chk', '__memcpy_chk', '__FD_ISSET_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
67	arm64-v8a/liblame.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.
68	arm64-v8a/libvorbis-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	False warning Symbols are available.
69	arm64-v8a/liblamemp3.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', '__vsprintf_chk']	False warning Symbols are available.
70	arm64-v8a/libsqlcipher.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
71	arm64-v8a/libogg.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.
72	arm64-v8a/libvorbis.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	21/24	android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.GET_TASKS, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.GET_ACCOUNTS, android.permission.READ_SMS, android.permission.RECEIVE_SMS, android.permission.READ_CALL_LOG, android.permission.READ_CONTACTS, android.permission.READ_PHONE_STATE, android.permission.VIBRATE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.RECORD_AUDIO, android.permission.WRITE_SETTINGS, android.permission.CAMERA, android.permission.SYSTEM_ALERT_WINDOW, android.permission.WAKE_LOCK

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	15/45	android.permission.FOREGROUND_SERVICE, android.permission.PACKAGE_USAGE_STATS, android.permission.CALL_PHONE, android.permission.PROCESS_OUTGOING_CALLS, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.READ_CALENDAR, android.permission.MODIFY_AUDIO_SETTINGS, com.android.launcher.permission.INSTALL_SHORTCUT, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.REQUEST_INSTALL_PACKAGES, android.permission.CHANGE_WIFI_STATE, android.permission.WRITE_CONTACTS, android.permission.FLASHLIGHT, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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

Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.icecast.org	ok	**IP:** 140.211.166.31 **Country:** United States of America **Region:** Oregon **City:** Eugene **Latitude:** 44.036083 **Longitude:** -123.052429 **View:** Google Map
emcpanel.com	ok	**IP:** 104.26.15.56 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

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
ikm-sv2.awsapi.io	ok	**IP:** 188.114.96.10 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
ikmws.awsapi.io	ok	**IP:** 188.114.97.10 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
ikm-sv3.awsapi.io	ok	No Geolocation information available.
pagead2.googlesyndication.com	ok	**IP:** 142.250.180.226 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ikmws-mirror.awsapi.io	ok	**IP:** 188.114.96.10 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
android.googlesource.com	ok	**IP:** 74.125.128.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
users.ikeymonitor.com	ok	**IP:** 172.66.43.145 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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
co4-client-s.gateway.messenger.live.com	ok	**IP:** 20.185.212.106 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map
www.openssl.org	ok	**IP:** 34.49.79.89 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 142.251.39.67 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
imo.im	ok	**IP:** 83.229.97.31 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Borehamwood **Latitude:** 51.654678 **Longitude:** -0.277620 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	**IP:** 142.250.180.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ikm-sv4.awsapi.io	ok	No Geolocation information available.
ikeymonitor.com	ok	**IP:** 172.66.40.111 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
support.ikeymonitor.com	ok	**IP:** 104.16.53.111 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com u0013android@android.com0	c2/u.java
g@groups.kik	d0/d.java

TRACKERS

TRACKER	CATEGORIES	URL
ACRA	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/444

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

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"key_preview_popup_dismiss_default_delay" : "Vaikeseade"
"prefs_enable_emoji_alt_physical_key_summary" : "□□Alt□□□□□□□□□□□□□□□□□□□□□□□□"
"key_preview_popup_dismiss_default_delay" : "Predvolené"
"key_preview_popup_dismiss_default_delay" : "Подразумевано"
"Reg_InCorrectLicKey" : "□□□□□"
"key_preview_popup_dismiss_default_delay" : "Standard"
"key_preview_popup_dismiss_default_delay" : "Predeterminado"
"key_preview_popup_dismiss_default_delay" : "■■■■■■■"
"key_preview_popup_dismiss_default_delay" : "Predefinido"
"key_preview_popup_dismiss_default_delay" : "Predeterminada"
"key_preview_popup_dismiss_no_delay" : "□□□"
"key_preview_popup_dismiss_default_delay" : "Privzeto"
"Lic_key_not_exist" : "□□□□□□□□"
"show_language_switch_key" : "□□□□□□□□"
"prefs_key_longpress_timeout_settings" : "□□□□□□□□"
"prefs_key_longpress_timeout_settings" : "□□□□□□"
"key_preview_popup_dismiss_default_delay" : "تلقائي"

POSSIBLE SECRETS
"key_preview_popup_dismiss_default_delay" : "Numatytasis"
"Debug_Licensekey" : "□□□□□□"
"enter_userName" : "□□□□□□"
"enter_userName" : "□□□□□□"
"Lic_key_not_exist" : "□□□□□□□□□"
"key_preview_popup_dismiss_delay" : "□□□□□□□□□"
"key_preview_popup_dismiss_default_delay" : "Default"
"show_language_switch_key_summary" : "□□□□□□□□□□□□□□□□□□"
"show_language_switch_key_summary" : "□□□□□□□□□□□□□□□□□□"
"Debug_Licensekey" : "Lizenzschlüssel"
"key_preview_popup_dismiss_default_delay" : "ნაგულისხმევი"
"show_language_switch_key" : "Sprachwechsel"
"key_preview_popup_dismiss_no_delay" : "□□□□□□"
"key_preview_popup_dismiss_default_delay" : "Padrão"
"Debug_Licensekey" : "□□□□□□□□"
"prefs_enable_emoji_alt_physical_key" : "□□□□□□□□□□□□□"
"show_language_switch_key" : "ปุ่มปรับภาษา"
"show_language_switch_key" : "□□□□□□"
"key_preview_popup_dismiss_delay" : "ไลยะเวลาภาบสะแดงไตอักสอบ"
"show_language_switch_key_summary" : "□□□□□□□□□□□□□"
"key_preview_popup_dismiss_default_delay" : "■■■■■■■■"
"key_preview_popup_dismiss_default_delay" : "Alapbeállítás"

POSSIBLE SECRETS
"prefs_key_longpress_timeout_settings" : "ໄລຍະເວລາຂອງການກົດປຸ່ມ"
"key_preview_popup_dismiss_default_delay" : "Predefinito"
"key_preview_popup_dismiss_default_delay" : "Oletus"
"key_preview_popup_dismiss_default_delay" : "Standart"
"prefs_key_longpress_timeout_settings" : "□□□□□□□"
"key_preview_popup_dismiss_no_delay" : "Kechikishsiz"
"deleted_key" : "%1$s□□□□□□□□"
"key_preview_popup_dismiss_default_delay" : "□□"
"enter_userName" : "Entr.NomUtilis"
"key_preview_popup_dismiss_delay" : "□□□□□□□□□□□□"
"show_language_switch_key_summary" : "□□□□□□□□□□□□□"
"key_preview_popup_dismiss_default_delay" : "ຄ່າເລີ່ມຕົ້ນ"
"key_preview_popup_dismiss_no_delay" : "Viivituseta"
"key_preview_popup_dismiss_default_delay" : "[redacted]"
"enter_userName" : "□□□□□□□□□□□□□"
"Reg_EnterLicKey" : "□□□□□□□□□□□□□□□□"
"key_preview_popup_dismiss_default_delay" : "Prestabilit"
"key_preview_popup_dismiss_default_delay" : "پیش‌فرض"
"prefs_enable_emoji_alt_physical_key" : "□□□□□□□□□□□□"
"show_language_switch_key" : "□□□□□"
"key_preview_popup_dismiss_default_delay" : "□□□"
"prefs_enable_emoji_alt_physical_key" : "□□□□□□□□□□□□□"

POSSIBLE SECRETS
"key_preview_popup_dismiss_default_delay" : "Noklusējums"
"key_preview_popup_dismiss_default_delay" : "□□□□□"
"key_preview_popup_dismiss_default_delay" : "Varsayılan"
"key_preview_popup_dismiss_default_delay" : "Chaguomsingi"
"show_language_switch_key_summary" : "ສະແດງໃນເວລາທີ່ຕົວເລືອກການປ້ອນຂໍ້ມູນຫຼາຍໂຕຖືກເປີດຢູ່"
"key_preview_popup_dismiss_no_delay" : "□□□"
"key_preview_popup_dismiss_delay" : "□□□□□□□□□□□□□"
"prefs_key_longpress_timeout_settings" : "□□□□□"
"Reg_InCorrectLicKey" : "□□□□□"
"Debug_Licensekey" : "□□□□□"
"show_language_switch_key" : "Kielenvaihtonäppäin"
"key_preview_popup_dismiss_default_delay" : "ڈیفالٹ"
"key_preview_popup_dismiss_default_delay" : "Προεπιλογή"
"key_preview_popup_dismiss_default_delay" : "Zadano"
"Reg_EnterLicKey" : "□□□□□□□□□□□□□□□□"
"Reg_InCorrectLicKey" : "□□□□□□□□□□□□□□□□□"
"key_preview_popup_dismiss_default_delay" : "Lehenetsia"
"key_preview_popup_dismiss_default_delay" : "Okuzenzakalelayo"
"key_preview_popup_dismiss_default_delay" : "□□"
"Lic_key_not_exist" : "□□□□□□□□□□□□□□□"
"prefs_enable_emoji_alt_physical_key" : "□□□□□□□□□□□□"
"key_preview_popup_dismiss_no_delay" : "ບໍ່ໃຊ້ໝົດເວລາ"

POSSIBLE SECRETS
"key_preview_popup_dismiss_delay" : "Tasten-Pop-up"
ccc707d2924768f2cc12bc8b
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa

SCAN LOGS

Timestamp	Event	Error
2024-08-10 18:51:41	Generating Hashes	OK
2024-08-10 18:51:41	Extracting APK	OK
2024-08-10 18:51:41	Unzipping	OK
2024-08-10 18:51:41	Getting Hardcoded Certificates/Keystores	OK
2024-08-10 18:51:43	Parsing AndroidManifest.xml	OK
2024-08-10 18:51:43	Parsing APK with androguard	OK
2024-08-10 18:51:44	Extracting Manifest Data	OK
2024-08-10 18:51:44	Performing Static Analysis on: Internet Service (com.sec.android.internet.im.service.im20210815)	OK
2024-08-10 18:51:44	Fetching Details from Play Store: com.sec.android.internet.im.service.im20210815	OK
2024-08-10 18:51:45	Manifest Analysis Started	OK

2024-08-10 18:51:45	Reading Network Security config from network_security_config.xml	OK
2024-08-10 18:51:45	Parsing Network Security config	OK
2024-08-10 18:51:45	Checking for Malware Permissions	OK
2024-08-10 18:51:45	Fetching icon path	OK
2024-08-10 18:51:45	Library Binary Analysis Started	OK
2024-08-10 18:51:45	Analyzing lib/armeabi-v7a/libresrtmp.so	OK
2024-08-10 18:51:45	Analyzing lib/armeabi-v7a/libwebpModule.so	OK
2024-08-10 18:51:45	Analyzing lib/armeabi-v7a/librestreaming.so	OK
2024-08-10 18:51:45	Analyzing lib/armeabi-v7a/libshout-jni.so	OK
2024-08-10 18:51:45	Analyzing lib/armeabi-v7a/liblamejni.so	OK
2024-08-10 18:51:45	Analyzing lib/armeabi-v7a/libshout.so	OK
2024-08-10 18:51:45	Analyzing lib/armeabi-v7a/liblame.so	OK
2024-08-10 18:51:46	Analyzing lib/armeabi-v7a/libvorbis-jni.so	OK
2024-08-10 18:51:46	Analyzing lib/armeabi-v7a/liblamemp3.so	OK
2024-08-10 18:51:46	Analyzing lib/armeabi-v7a/libsqlcipher.so	OK

2024-08-10 18:51:48	Analyzing lib/armeabi-v7a/libogg.so	OK
2024-08-10 18:51:48	Analyzing lib/armeabi-v7a/libvorbis.so	OK
2024-08-10 18:51:48	Analyzing lib/x86_64/libresrtmp.so	OK
2024-08-10 18:51:48	Analyzing lib/x86_64/libwebpModule.so	OK
2024-08-10 18:51:48	Analyzing lib/x86_64/librestreaming.so	OK
2024-08-10 18:51:48	Analyzing lib/x86_64/libshout-jni.so	OK
2024-08-10 18:51:48	Analyzing lib/x86_64/liblamejni.so	OK
2024-08-10 18:51:48	Analyzing lib/x86_64/libshout.so	OK
2024-08-10 18:51:48	Analyzing lib/x86_64/liblame.so	OK
2024-08-10 18:51:48	Analyzing lib/x86_64/libvorbis-jni.so	OK
2024-08-10 18:51:49	Analyzing lib/x86_64/liblamemp3.so	OK
2024-08-10 18:51:49	Analyzing lib/x86_64/libsqlcipher.so	OK
2024-08-10 18:51:50	Analyzing lib/x86_64/libogg.so	OK
2024-08-10 18:51:51	Analyzing lib/x86_64/libvorbis.so	OK
2024-08-10 18:51:51	Analyzing lib/arm64-v8a/libresrtmp.so	OK

2024-08-10 18:51:51	Analyzing lib/arm64-v8a/libwebpModule.so	OK
2024-08-10 18:51:51	Analyzing lib/arm64-v8a/librestreaming.so	OK
2024-08-10 18:51:51	Analyzing lib/arm64-v8a/libshout-jni.so	OK
2024-08-10 18:51:51	Analyzing lib/arm64-v8a/liblamejni.so	OK
2024-08-10 18:51:51	Analyzing lib/arm64-v8a/libshout.so	OK
2024-08-10 18:51:51	Analyzing lib/arm64-v8a/liblame.so	OK
2024-08-10 18:51:51	Analyzing lib/arm64-v8a/libvorbis-jni.so	OK
2024-08-10 18:51:52	Analyzing lib/arm64-v8a/liblamemp3.so	OK
2024-08-10 18:51:52	Analyzing lib/arm64-v8a/libsqlcipher.so	OK
2024-08-10 18:51:54	Analyzing lib/arm64-v8a/libogg.so	OK
2024-08-10 18:51:54	Analyzing lib/arm64-v8a/libvorbis.so	OK
2024-08-10 18:51:54	Analyzing apktool_out/lib/armeabi-v7a/libresrtmp.so	OK
2024-08-10 18:51:54	Analyzing apktool_out/lib/armeabi-v7a/libwebpModule.so	OK
2024-08-10 18:51:54	Analyzing apktool_out/lib/armeabi-v7a/librestreaming.so	OK
2024-08-10 18:51:54	Analyzing apktool_out/lib/armeabi-v7a/libshout-jni.so	OK

2024-08-10 18:51:54	Analyzing apktool_out/lib/armeabi-v7a/liblamejni.so	OK
2024-08-10 18:51:54	Analyzing apktool_out/lib/armeabi-v7a/libshout.so	OK
2024-08-10 18:51:54	Analyzing apktool_out/lib/armeabi-v7a/liblame.so	OK
2024-08-10 18:51:55	Analyzing apktool_out/lib/armeabi-v7a/libvorbis-jni.so	OK
2024-08-10 18:51:55	Analyzing apktool_out/lib/armeabi-v7a/liblamemp3.so	OK
2024-08-10 18:51:55	Analyzing apktool_out/lib/armeabi-v7a/libsqlcipher.so	OK
2024-08-10 18:51:57	Analyzing apktool_out/lib/armeabi-v7a/libogg.so	OK
2024-08-10 18:51:57	Analyzing apktool_out/lib/armeabi-v7a/libvorbis.so	OK
2024-08-10 18:51:57	Analyzing apktool_out/lib/x86_64/libresrtmp.so	OK
2024-08-10 18:51:57	Analyzing apktool_out/lib/x86_64/libwebpModule.so	OK
2024-08-10 18:51:57	Analyzing apktool_out/lib/x86_64/librestreaming.so	OK
2024-08-10 18:51:57	Analyzing apktool_out/lib/x86_64/libshout-jni.so	OK
2024-08-10 18:51:57	Analyzing apktool_out/lib/x86_64/liblamejni.so	OK
2024-08-10 18:51:57	Analyzing apktool_out/lib/x86_64/libshout.so	OK
2024-08-10 18:51:57	Analyzing apktool_out/lib/x86_64/liblame.so	OK

2024-08-10 18:51:58	Analyzing apktool_out/lib/x86_64/libvorbis-jni.so	OK
2024-08-10 18:51:58	Analyzing apktool_out/lib/x86_64/liblamemp3.so	OK
2024-08-10 18:51:58	Analyzing apktool_out/lib/x86_64/libsqlcipher.so	OK
2024-08-10 18:52:00	Analyzing apktool_out/lib/x86_64/libogg.so	OK
2024-08-10 18:52:00	Analyzing apktool_out/lib/x86_64/libvorbis.so	OK
2024-08-10 18:52:00	Analyzing apktool_out/lib/arm64-v8a/libresrtmp.so	OK
2024-08-10 18:52:00	Analyzing apktool_out/lib/arm64-v8a/libwebpModule.so	OK
2024-08-10 18:52:00	Analyzing apktool_out/lib/arm64-v8a/librestreaming.so	OK
2024-08-10 18:52:00	Analyzing apktool_out/lib/arm64-v8a/libshout-jni.so	OK
2024-08-10 18:52:00	Analyzing apktool_out/lib/arm64-v8a/liblamejni.so	OK
2024-08-10 18:52:00	Analyzing apktool_out/lib/arm64-v8a/libshout.so	OK
2024-08-10 18:52:01	Analyzing apktool_out/lib/arm64-v8a/liblame.so	OK
2024-08-10 18:52:01	Analyzing apktool_out/lib/arm64-v8a/libvorbis-jni.so	OK
2024-08-10 18:52:01	Analyzing apktool_out/lib/arm64-v8a/liblamemp3.so	OK
2024-08-10 18:52:01	Analyzing apktool_out/lib/arm64-v8a/libsqlcipher.so	OK

2024-08-10 18:52:03	Analyzing apktool_out/lib/arm64-v8a/libogg.so	OK
2024-08-10 18:52:03	Analyzing apktool_out/lib/arm64-v8a/libvorbis.so	OK
2024-08-10 18:52:03	Reading Code Signing Certificate	OK
2024-08-10 18:52:03	Running APKiD 2.1.5	OK
2024-08-10 18:52:06	Detecting Trackers	OK
2024-08-10 18:52:07	Decompiling APK to Java with jadx	OK
2024-08-10 18:52:22	Converting DEX to Smali	OK
2024-08-10 18:52:22	Code Analysis Started on - java_source	OK
2024-08-10 18:52:32	Android SAST Completed	OK
2024-08-10 18:52:32	Android API Analysis Started	OK
2024-08-10 18:52:44	Android Permission Mapping Started	OK
2024-08-10 18:54:41	Android Permission Mapping Completed	OK
2024-08-10 18:54:42	Finished Code Analysis, Email and URL Extraction	OK
2024-08-10 18:54:42	Extracting String data from APK	OK
2024-08-10 18:54:42	Extracting String data from SO	OK

2024-08-10 18:54:43	Extracting String data from Code	OK
2024-08-10 18:54:43	Extracting String values and entropies from Code	OK
2024-08-10 18:54:44	Performing Malware check on extracted domains	OK
2024-08-10 18:54:49	Saving to Database	OK
