MOBSF

ANDROID STATIC ANALYSIS REPORT

ReverseHand (1.0.0)

File Name:	app-release.apk
Package Name:	reversehand.app.app
Scan Date:	Sept. 21, 2022, 8:13 a.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/428

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	12	2	2	1

FILE INFORMATION

File Name: app-release.apk
Size: 99.53MB
MD5: bcfdf63dca5c06207cb8e88e6f34e117
SHA1: 2a24a9710db480d79fbb25b1b6f0cc422208d99c
SHA256: e6acb474a04a29b01d5142ff1174a2aadd67b8c83544254cd038463d975d54df

APP INFORMATION

App Name: ReverseHand
Package Name: reversehand.app.app
Main Activity: reversehand.app.app.MainActivity
Target SDK: 31
Min SDK: 23
Max SDK:
Android Version Name: 1.0.0
Android Version Code: 1

APP COMPONENTS

Activities: 10
Services: 4
Receivers: 0
Providers: 1
Exported Activities: 1
Exported Services: 1
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=za, ST=Gauteng, L=Pretoria, O=ReverseHand, OU=Cache Money, CN=Alexander Muendesi
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-09-21 07:37:25+00:00
Valid To: 2047-09-15 07:37:25+00:00
Issuer: C=za, ST=Gauteng, L=Pretoria, O=ReverseHand, OU=Cache Money, CN=Alexander Muendesi
Serial Number: 0x3224bf38
Hash Algorithm: sha256
md5: 5ae359887840a5a087846d0e8be1ca62
sha1: a0eb643e3452deb787a3e59dd9d3cec9535c8343
sha256: 6ea64afecafb684b88c1e9166879c2a955cbb12b38c847b2b4b55cba3b8b503b
sha512: f4f659d66eccac4572d428e21e15dc6e2e9418939f68f889da4e928242cd51c80a48fda8760ebd7221c473d0ca521ed14d660fd93b6a1588485eb6c612bcdc03
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: dd7737cd5ec00a98575da1ed78249540cbeba0ae4593f176e74cff1e495eef2f

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.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

APKID ANALYSIS

FILE	DETAILS
classes.dex	<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.TAGS check network operator name check possible VM check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.amplifyframework.auth.cognito.activities.HostedUIRedirectActivity	Schemes: reversehandapp://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
2	Activity (com.amplifyframework.auth.cognito.activities.HostedUIRedirectActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
3	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				co/paystack/flutterpaystack/a.java co/paystack/flutterpaystack/b.java com/amazonaws/amplify/Amplify.java com/amazonaws/amplify/amplify_storage_s3/StorageS3.java com/amazonaws/cognito/clientcontext/data/UserContextDataProvider.java com/amazonaws/cognito/clientcontext/datacollection/ApplicationDataCollector.java com/amazonaws/cognito/clientcontext/util/SignatureGenerator.java com/amazonaws/logging/AndroidLog.java com/amazonaws/logging/ConsoleLog.java com/amazonaws/mobile/auth/core/DefaultSignInResultHandler.java

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	com/amazonaws/mobile/auth/core/IdentityManager.java com/amazonaws/mobile/auth/core/signin/SignInManager.java com/amazonaws/mobile/client/AWSMobileClient.java com/amazonaws/mobile/client/activities/HostedUIRedirectActivity.java com/amazonaws/mobile/client/internal/InternalCallback.java com/amazonaws/mobile/client/internal/oauth2/OAuth2Client.java com/amazonaws/mobileconnectors/cognitoauth/AuthClient.java com/amazonaws/mobileconnectors/cognitoauth/activities/CustomTabsManagerActivity.java com/amazonaws/mobileconnectors/cognitoauth/util/LocalDataManager.java com/amazonaws/mobileconnectors/cognitoidentityprovider/CognitoUserSession.java com/amazonaws/mobileconnectors/pinpoint/targeting/notification/EventSourceType.java com/amplifyframework/analytics/pinpoint/AutoSessionTracker.java com/amplifyframework/logging/AndroidLogger.java com/amplifyframework/logging/JavaLogger.java com/baseflow/geolocator/GeolocatorLocationService.java com/baseflow/geolocator/m.java com/baseflow/geolocator/n.java com/baseflow/geolocator/o.java com/baseflow/geolocator/q/j.java com/baseflow/geolocator/r/b.java com/mr/flutter/plugin/filepicker/b.java com/mr/flutter/plugin/filepicker/c.java com/shockwave/pdfium/PdfiumCore.java e/a/k/a/a.java e/a/n/g.java e/c/b/c.java e/f/b/k/f.java e/h/d/e/a.java

e/h/d/e/b.java
e/h/d/e/f.java
e/h/e/c.java
e/h/e/e.java
e/h/e/f.java
e/h/e/g.java
e/h/e/j.java
e/h/e/k.java
e/h/h/d.java
e/h/j/b.java
e/h/k/c.java
e/h/l/a0.java
e/h/l/b.java
e/h/l/c0/c.java
e/h/l/f.java
e/h/l/h.java
e/h/l/s.java
e/h/l/t.java
e/h/l/v.java
e/j/b/d.java
e/k/a/a.java
e/n/a/b.java
e/q/i0.java
e/q/y.java
e/r/a/a/h.java
f/a/a/a/e.java
f/a/a/a/h.java
f/a/a/a/j/a.java
f/b/a/a/b/d.java
f/b/a/a/b/g.java
f/b/a/a/b/h.java
f/b/a/a/b/k/a.java
f/b/a/a/b/o.java
f/b/a/a/b/p.java
f/b/a/a/d/c/r.java
f/b/a/a/e/b/a.java
f/b/a/b/a0/g.java
f/b/a/b/l/h.java
f/b/a/b/n/a.java
f/b/a/b/x/d.java
f/b/a/b/y/b.java
f/b/a/c/a/b/a.java

				f/b/a/c/a/b/y.java h/b/b.java io/flutter/plugins/b/a.java io/flutter/plugins/imagepicker/b.java io/flutter/plugins/imagepicker/g.java k/k0/b.java k/k0/j/i/c.java
2	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/amazonaws/services/s3/internal/MD5DigestCalculatingInputStream.java com/amazonaws/util/Md5Utils.java
				com/amazonaws/amplify/amplify_api/FlutterApiRequest.java com/amazonaws/amplify/amplify_auth_cognito/device/DeviceKt.java com/amazonaws/auth/CognitoCachingCredentialsProvider.java com/amazonaws/auth/policy/conditions/ConditionFactory.java com/amazonaws/auth/policy/conditions/S3ConditionFactory.java com/amazonaws/cognito/clientcontext/data/UserContextDataProvider.java com/amazonaws/cognito/clientcontext/datacollection/DeviceDataCollector.java com/amazonaws/internal/keyvaluestore/AWSKeyValueStore.java com/amazonaws/internal/keyvaluestore/KeyProvider18.java com/amazonaws/mobile/auth/core/IdentityManager.java com/amazonaws/mobile/client/AWSMobileClient.java com/amazonaws/mobile/client/internal/oauth2/OAuth2Client.java com/amazonaws/mobileconnectors/cognitoauth/activities/CustomTabsManagerActivity.java com/amazonaws/mobileconnectors/cognitoidentityprovider/util/CognitoDeviceHelper.java

3	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/amazonaws/mobileconnectors/cognitoidentityprovider/util/CognitoPinpointSharedContext.java com/amazonaws/mobileconnectors/cognitoidentityprovider/util/CognitoServiceConstants.java com/amazonaws/mobileconnectors/pinpoint/analytics/SessionClient.java com/amazonaws/mobileconnectors/pinpoint/internal/core/configuration/AndroidPreferencesConfiguration.java com/amazonaws/mobileconnectors/pinpoint/internal/core/idresolver/SharedPrefsUniqueIdService.java com/amazonaws/mobileconnectors/pinpoint/internal/event/ClientContext.java com/amazonaws/mobileconnectors/pinpoint/internal/event/EventRecorder.java com/amazonaws/mobileconnectors/pinpoint/targeting/TargetingClient.java com/amazonaws/mobileconnectors/pinpoint/targeting/notification/EventSourceType.java com/amazonaws/mobileconnectors/pinpoint/targeting/notification/NotificationClient.java com/amazonaws/mobileconnectors/pinpoint/targeting/notification/NotificationClientBase.java com/amazonaws/mobileconnectors/s3/transferutility/TransferObserver.java com/amazonaws/mobileconnectors/s3/transferutility/TransferTable.java com/amazonaws/services/s3/Headers.java com/amazonaws/services/s3/model/S3ObjectSummary.java com/amplifyframework/analytics/pinpoint/AWSPinpointAnalyticsPlugin.java com/amplifyframework/api/aws/ApiGraphQLRequestOptions.java com/amplifyframework/api/aws/GsonGraphQLResponseFactory.java com/amplifyframework/api/aws/SubscriptionAuthorizer.java com/amplifyframework/api/aws/auth/ApiKeyRequestDecorator.java com/amplifyframework/api/aws/auth/ApiRequestD

				ecoratorFactory.java com/amplifyframework/api/aws/sigv4/DefaultCognitoUserPoolsAuthProvider.java com/amplifyframework/api/graphql/GsonResponseAdapters.java com/amplifyframework/auth/AuthProvider.java com/amplifyframework/auth/AuthUser.java com/amplifyframework/auth/AuthUserAttribute.java com/amplifyframework/auth/AuthUserAttributeKey.java com/amplifyframework/auth/cognito/AWSCognitoAuthPlugin.java com/amplifyframework/core/category/CategoryConfiguration.java com/amplifyframework/datastore/appsync/AppSyncExtensions.java com/amplifyframework/datastore/appsync/ModelWithMetadataAdapter.java com/amplifyframework/storage/StorageItem.java com/amplifyframework/storage/s3/AWSMobileClientAuthProvider.java com/amplifyframework/storage/s3/AWSS3StoragePlugin.java e/c/b/b.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	com/amazonaws/mobileconnectors/pinpoint/targeting/notification/NotificationClientBase.java com/amazonaws/retry/PredefinedRetryPolicies.java i/w/a.java i/w/b.java i/w/d/a.java k/a0.java k/k0/m/d.java k/k0/m/h.java
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/mr/flutter/plugin/filepicker/b.java com/mr/flutter/plugin/filepicker/c.java e/h/d/a.java e/h/d/b.java io/flutter/plugins/b/a.java

6	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/amplifyframework/devmenu/DeveloperMenu.java io/flutter/plugin/editing/b.java io/flutter/plugin/platform/g.java
7	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/amazonaws/mobileconnectors/pinpoint/internal/event/EventTable.java com/amazonaws/mobileconnectors/pinpoint/internal/event/PinpointDBBase.java com/amazonaws/mobileconnectors/pinpoint/internal/event/PinpointDatabaseHelper.java com/amazonaws/mobileconnectors/s3/transferutility/TransferTable.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	com/amazonaws/mobileconnectors/s3/transferutility/TransferUtility.java e/k/a/a.java io/flutter/plugins/imagepicker/c.java io/flutter/plugins/imagepicker/e.java
9	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	k/k0/j/c.java k/k0/j/d.java k/k0/j/g.java k/k0/j/h.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	f/b/a/c/a/b/o.java
11	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/amazonaws/mobileconnectors/cognitoidentityprovider/CognitoUser.java com/amazonaws/mobileconnectors/cognitoidentityprovider/util/CognitoDeviceHelper.java
12	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	co/paystack/flutterpaystack/AuthActivity.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/armeabi-v7a/libflutter.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
2	lib/armeabi-v7a/libapp.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
		True info The shared object has NX	True info This shared object has a stack canary value added to	None info The shared	None info The shared object does	False warning The shared object does not have any fortified	True info Symbols are stripped.

3	lib/armeabi-v7a/libjniPdfium.so	bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	object does not have run-time search path or RPATH set.	not have RUNPATH set.	functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	
4	lib/armeabi-v7a/libmodpng.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
5	lib/armeabi-v7a/libmodpdfium.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
		True info The shared	True info This shared object has a	None info The	None info The shared	False warning The shared object does	True info Symbols are

6	lib/armeabi-v7a/libc++_shared.so	object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	shared object does not have run-time search path or RPATH set.	object does not have RUNPATH set.	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.	stripped.
7	lib/armeabi-v7a/libmodft2.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
8	lib/x86/libjniPdfium.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
		True info	True info	None info	None info	False warning	True info

9	lib/x86/libmodpng.so	The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	This shared object 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.	The shared object does not have run-time search path or RPATH set.	The shared object does not have RUNPATH set.	The shared object 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.	Symbols are stripped.
10	lib/x86/libmodpdfium.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
11	lib/x86/libc++_shared.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.

12	lib/x86/libmodft2.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
13	lib/x86_64/libflutter.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__strncpy_chk', '__memmove_chk']	True info Symbols are stripped.
14	lib/x86_64/libapp.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.

15	lib/x86_64/libjniPdfium.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
16	lib/x86_64/libmodpng.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk']	True info Symbols are stripped.
17	lib/x86_64/libmodpdfium.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk', '__snprintf_chk', '__strchr_chk', '__vsnprintf_chk', '__read_chk', '__sprintf_chk']	True info Symbols are stripped.

		executable.					
18	lib/x86_64/libc++_shared.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
19	lib/x86_64/libmodft2.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strcat_chk', '__strlen_chk', '__strrchr_chk']	True info Symbols are stripped.
20	lib/arm64-v8a/libflutter.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected	False high This shared object 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.	None info The shared object does not have run-time search path or RPATH	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__strncpy_chk',	True info Symbols are stripped.

		shellcode non-executable.		set.		'__memmove_chk']	
21	lib/arm64-v8a/libapp.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
22	lib/arm64-v8a/libjniPdfium.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
23	lib/arm64-v8a/libmodpng.so	True info The shared object has NX bit set. This marks a memory page non-executable making	True info This shared object 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	None info The shared object does not have run-time search	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk']	True info Symbols are stripped.

		attacker injected shellcode non-executable.	verifying the integrity of the canary before function return.	path or RPATH set.			
24	lib/arm64-v8a/libmodpdfium.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk', '__snprintf_chk', '__strchr_chk', '__vsnprintf_chk', '__read_chk', '__sprintf_chk']	True info Symbols are stripped.
25	lib/arm64-v8a/libc++_shared.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
26	lib/arm64-v8a/libmodft2.so	True info The shared object has NX bit set. This marks a memory page	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the	None info The shared object does not have	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strcat_chk', '__strlen_chk', '__strrchr_chk']	True info Symbols are stripped.

		non-executable making attacker injected shellcode non-executable.	return address. This allows detection of overflows by verifying the integrity of the canary before function return.	run-time search path or RPATH set.			
27	lib/mips/libjniPdfium.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
28	lib/mips/libmodpng.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
		True info The shared object has NX bit set. This	True info This shared object has a stack canary value added to the stack so that it will be	None info The shared object	None info The shared object does not have	False warning The shared object does not have any fortified functions. Fortified	True info Symbols are stripped.

29	lib/mips/libmodpdfium.so	marks a memory page non-executable making attacker injected shellcode non-executable.	overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	does not have run-time search path or RPATH set.	RUNPATH set.	functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	
30	lib/mips/libc++_shared.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
31	lib/mips/libmodft2.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object 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.	True info Symbols are stripped.
		True info The shared object has NX	True info This shared object has a stack canary value added to	None info The shared	None info The shared object does	False warning The shared object does not have any fortified	True info Symbols are stripped.

32	lib/mips64/libjniPdfium.so	bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	object does not have run-time search path or RPATH set.	not have RUNPATH set.	functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	
33	lib/mips64/libmodpng.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk']	True info Symbols are stripped.
34	lib/mips64/libmodpdfium.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__read_chk', '__strlen_chk', '__snprintf_chk', '__sprintf_chk', '__strchr_chk', '__vsnprintf_chk', '_chk', 'en_chk', 'strlen_chk', 'en_chk', 'strlen_chk', 'd_chk', 'strlen_chk']	True info Symbols are stripped.
		True info The shared	True info This shared object has a	None info The	None info The shared	False warning The shared object does	True info Symbols are

35	lib/mips64/libc++_shared.so	object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	shared object does not have run-time search path or RPATH set.	object does not have RUNPATH set.	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.	stripped.
36	lib/mips64/libmodft2.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__strlen_chk', '__strrchr_chk', '__strcat_chk', 'strcat_chk']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.

3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['location', 'network connectivity'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.

12	FCS_COP.1.1(4)	Selection-Based Security Functional Requirements	Cryptographic Operation - Keyed-Hash Message Authentication	The application perform keyed-hash message authentication with cryptographic algorithm ['HMAC-SHA-256'] .
13	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
14	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
15	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
16	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
17	FCS_CKM.1.1(2)	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
api.flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991

		Longitude: -122.078514 **View:** Google Map
standard.paystack.co	ok	**IP:** 104.17.190.8 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
docs.amplify.aws	ok	**IP:** 52.85.254.80 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
s3-us-west-1.amazonaws.com	ok	**IP:** 52.219.116.16 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
api.paystack.co	ok	**IP:** 104.17.191.8 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700

		Longitude: -122.395203 **View:** Google Map
developer.android.com	ok	**IP:** 172.217.170.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.w3.org	ok	**IP:** 128.30.52.100 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.365078 **Longitude:** -71.104523 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
www.amazon.com	ok	**IP:** 52.85.217.44 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
		IP: 172.217.170.74 **Country:** United States of America

maps.googleapis.com	ok	**Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
www.ngs.ac.uk	ok	**IP:** 130.246.140.235 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Appleton **Latitude:** 51.709511 **Longitude:** -1.361360 **View:** Google Map
s3.amazonaws.com	ok	**IP:** 54.231.230.240 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
acs.amazonaws.com	ok	No Geolocation information available.

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	f/b/a/a/b/u.java
_cookie@13463476.fromsetcoo authenticationscheme@13463476.fromstring _list@0150898.of _httpparser@13463476.responsepa lectiontoolbarbutton@868113492.text _list@0150898.generate n_typeerror@0150898._create _list@0150898._ofgrowabl omdp0101@gmail.com _list@0150898._ofefficie _growablelist@0150898._ofarray _double@0150898.fromintege _growablelist@0150898._literal3 ._future@4048458.immediate _growablelist@0150898._literal u_growablelist@0150898._ofother _link@14069316.fromrawpat c_growablelist@0150898.withcapaci _future@4048458.value _timer@1026248._internal _growablelist@0150898._literal6 _growablelist@0150898._literal5 _rawsocket@14069316._readpipe _receiveportimpl@1026248.fromrawrec -_list@0150898._ofarray _socket@14069316._readpipe z_timer@1026248.periodic m_growablelist@0150898._literal2 _list@0150898.empty storationinformation@1159124995.fromserial _list@0150898._ofother eo_bytebuffer@7027147._new _directory@14069316.fromrawpat _casterror@0150898._create l_invocationmirror@0150898._withtype _colorfilter@16065589.mode	lib/armeabi-v7a/libapp.so

ngstreamsubscription@4048458.zoned _assertionerror@0150898._create _colorfilter@16065589.srgbtoline lectiontoolbarbutton@747392285.text i_rawsocket@14069316._writepipe av_nativesocket@14069316.normal 4_uri@0150898.file _growablelist@0150898._literal1 _uri@0150898.directory q_imagefilter@16065589.blur qd_growablelist@0150898._literal8 v_file@14069316.fromrawpat _growablelist@0150898._literal4 bb_growablelist@0150898._ofgrowabl x_growablelist@0150898.of gh_growablelist@0150898.generate _uri@0150898.notsimple 7u_growablelist@0150898._literal7 _future@4048458.zonevalue k_colorfilter@16065589.lineartosr __growablelist@0150898._ofefficie _future@4048458.immediatee _nativesocket@14069316.pipe	
appro@openssl.org	lib/arm64-v8a/libflutter.so

TRACKERS

TRACKER	CATEGORIES	URL
Amazon Analytics (Amazon insights)	Analytics	https://reports.exodus-privacy.eu.org/trackers/95
Amazon Mobile Analytics (Amplify)	Analytics	https://reports.exodus-privacy.eu.org/trackers/423

Report Generated by - MobSF v3.5.2 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.