ANDROID STATIC ANALYSIS REPORT

Lite (376.0.0.7.103)

File Name:	facebook_lite_v376.0.0.7.103.apk
Package Name:	com.facebook.lite
Scan Date:	Oct. 25, 2023, 4:42 a.m.
App Security Score:	12/100 (CRITICAL RISK)
Grade:	F

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
53	9	1	3	1

FILE INFORMATION

File Name: facebook_lite_v376.0.0.7.103.apk
Size: 2.44MB
MD5: cbbe2a2afdbd78a6072eb8dd302b31df
SHA1: 335eaf3d341e614f305d8d2496de713b1092d294
SHA256: a735d7a5052a35dddf332a8cfafb40b52cfed1899a354fa97c16ee37c7b2ac00

APP INFORMATION

App Name: Lite
Package Name: com.facebook.lite
Main Activity: com.facebook.lite.MainActivity
Target SDK: 33
Min SDK: 15
Max SDK:
Android Version Name: 376.0.0.7.103
Android Version Code: 501001157

APP COMPONENTS

Activities: 17
Services: 35
Receivers: 32
Providers: 9
Exported Activities: 30
Exported Services: 2
Exported Receivers: 11
Exported Providers: 4

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=US, ST=CA, L=Palo Alto, O=Facebook Mobile, OU=Facebook, CN=Facebook Corporation
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2009-08-31 21:52:16+00:00
Valid To: 2050-09-25 21:52:16+00:00
Issuer: C=US, ST=CA, L=Palo Alto, O=Facebook Mobile, OU=Facebook, CN=Facebook Corporation
Serial Number: 0x4a9c4610
Hash Algorithm: md5
md5: 3fad024f2dcbe3ee693c96f350f8e376
sha1: 8a3c4b262d721acd49a4bf97d5213199c86fa2b9
sha256: e3f9e1e0cf99d0e56a055ba65e241b3399f7cea524326b0cdd6ec1327ed0fdc1
sha512: cd0c5bea15efd4c2620b5632a2d7618bc1cffb2edfc0f70e2f03ce593c162a93f655771bb2e222238889d4a5740f3dcbcd5b14b8a266602048500c67b0f07d14
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: f399a11f1d0ba109236e9b0cd20c7384a55d02042ba6c2500cec5a0001e165a1
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.BATTERY_STATS	signature	modify battery statistics	Allows the modification of collected battery statistics. Not for use by common applications.
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
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.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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
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_PHONE_NUMBERS	dangerous		Allows read access to the device's phone number(s). This is a subset of the capabilities granted by READ_PHONE_STATE but is exposed to instant applications.
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	dangerous		Allows an application to read image or video files from external storage that a user has selected via the permission prompt photo picker. Apps can check this permission to verify that a user has decided to use the photo picker, instead of granting access to READ_MEDIA_IMAGES or READ_MEDIA_VIDEO . It does not prevent apps from accessing the standard photo picker manually. This permission should be requested alongside READ_MEDIA_IMAGES and/or READ_MEDIA_VIDEO , depending on which type of media is desired.
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.facebook.receiver.permission.ACCESS	unknown	Unknown permission	Unknown permission from android reference
com.facebook.katana.provider.ACCESS	unknown	Unknown permission	Unknown permission from android reference
com.facebook.orca.provider.ACCESS	unknown	Unknown permission	Unknown permission from android reference
com.facebook.mlite.provider.ACCESS	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.facebook.wakizashi.provider.ACCESS	unknown	Unknown permission	Unknown permission from android reference
com.facebook.permission.prod.FB_APP_COMMUNICATION	unknown	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.WRITE	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.READ	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.oppo.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.
android.permission.USE_FULL_SCREEN_INTENT	normal		Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.BIND_NOTIFICATION_LISTENER_SERVICE	signature		Must be required by an NotificationListenerService, to ensure that only the system can bind to it.
com.facebook.services.identity.FEO2	unknown	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal		Allows a regular application to use Service.startForeground with the type "dataSync".
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.facebook.lite.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.SCHEDULE_EXACT_ALARM	normal		Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.READ_MEDIA_IMAGES	dangerous		Allows an application to read image files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous		Allows an application to read video files from external storage.
android.permission.POST_NOTIFICATIONS	dangerous		Allows an app to post notifications
com.google.android.gms.permission.AD_ID	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ANSWER_PHONE_CALLS	dangerous		Allows the app to answer an incoming phone call.
android.permission.READ_CALL_LOG	dangerous		Allows an application to read the user's call log.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.facebook.lite.MainActivity	Schemes: fblite://, Mime Types: text/plain,

ACTIVITY	INTENT
com.facebook.lite.deeplinking.activities.PermalinkPossiblePatternsActivityAlias	Schemes: http://, https://, Hosts: www.facebook.com, m.facebook.com, Paths: /permalink.php, /story.php, /home.php, /photo.php, /video.php, /n/, /nd/, Path Prefixes: /share, /events, /groups, /watch, /marketplace, /coronavirus_info, /mobile_center, /pages, /uiqr/.*, /fbrdr/2048/, /fbrdr/274/, /profile.php, Path Patterns: /.*/videos/.*, /reel/.*, /places/..*/..*, /.*/posts/.*, /.*/photos/.*, /.*/photos, /.*/media_set, /.*/about, /.*/photos_of, /.*/photos_albums, /.*/friends, /inter_app/redirect/.*, /privacy_access_hub/.*, /contact_upload_settings/.*, /pg/.*/home, /pg/.*/home/, /pg/.*/about, /pg/.*/about/, /pg/.*/photos, /pg/.*/photos/, /pages/whatsapp, /pages, /fblite_transfer_your_information/.*, /dogfooding_assistant,
com.facebook.lite.deeplinking.activities.PermalinkFBLinksAlias	Schemes: fb://,
com.facebook.lite.deeplinking.UIQRE2EActivity	Schemes: uiqr://,
com.facebook.lite.deeplinking.activities.PermalinkLiteActivityAlias	Schemes: http://, https://, Hosts: www.facebook.com, m.facebook.com, fb.com, Path Prefixes: /lite, /fblite/launch, /ema/install,
com.facebook.lite.deeplinking.activities.PermalinkWatchShortAlias	Schemes: http://, https://, Hosts: fb.watch, fbwat.ch, Path Patterns: /.*,
com.facebook.lite.deeplinking.activities.PermalinkFbliteMessagingFbMePrefixAlias	Schemes: http://, https://, Hosts: fb.me, Path Patterns: /.*,
com.facebook.lite.deeplinking.activities.CommunityChatsMDotMePrefixAlias	Schemes: http://, https://, Hosts: m.me, Path Patterns: /.*,

ACTIVITY	INTENT
com.facebook.lite.deeplinking.activities.PermalinkVanityPrefixAt	Schemes: http://, https://, Hosts: www.facebook.com, m.facebook.com, Path Patterns: /@.*,
com.facebook.lite.deeplinking.activities.PermalinkVanityPrefixP	Schemes: http://, https://, Hosts: www.facebook.com, m.facebook.com, Path Patterns: /p/.*,
com.facebook.lite.deeplinking.activities.PermalinkVanityPrefixTilde	Schemes: http://, https://, Hosts: www.facebook.com, m.facebook.com, Path Patterns: /~.*,
com.facebook.lite.deeplinking.activities.PermalinkHomeAlias	Schemes: http://, https://, Hosts: www.facebook.com, m.facebook.com, Paths: /,
com.facebook.lite.deeplinking.activities.PermalinkMessagingAlias	Schemes: http://, https://, Hosts: www.facebook.com, m.facebook.com, Path Patterns: /messages, /messages/read, /messages/t/.*,
com.facebook.lite.deeplinking.activities.PermalinkSettingsAlias	Schemes: http://, https://, Hosts: www.facebook.com, m.facebook.com, Path Prefixes: /settings,
com.facebook.lite.deeplinking.activities.PermalinkTimelineAlias	Schemes: http://, https://, Hosts: www.facebook.com, m.facebook.com, Path Prefixes: /timeline,
com.facebook.lite.deeplinking.activities.PermalinkNotificationsAlias	Schemes: http://, https://, Hosts: www.facebook.com, m.facebook.com, Path Prefixes: /notifications,

ACTIVITY	INTENT
com.facebook.lite.deeplinking.activities.PermalinkProfileEditAlias	Schemes: http://, https://, Hosts: www.facebook.com, m.facebook.com, Path Prefixes: /profile/edit,
com.facebook.lite.deeplinking.activities.PermalinkBuddylistAlias	Schemes: http://, https://, Hosts: www.facebook.com, m.facebook.com, Paths: /buddylist.php,
com.facebook.lite.deeplinking.activities.PermalinkExtraFacebookHostsAlias	Schemes: http://, https://, Hosts: facebook.com, fb.com, free.facebook.com, m.alpha.facebook.com, m.beta.facebook.com, mbasic.alpha.facebook.com, mbasic.beta.facebook.com, mbasic.facebook.com, mobile.facebook.com, mtouch.facebook.com, p.facebook.com, touch.facebook.com, web.facebook.com, www.alpha.facebook.com, www.beta.facebook.com, x.facebook.com, Paths: /permalink.php, /story.php, /home.php, /photo.php, /video.php, /n/, /nd/, Path Prefixes: /events, /groups, /watch, /marketplace, /coronavirus_info, /mobile_center, /pages, /uiqr/.*, /fbrdr/2048/, /fbrdr/274/, /profile.php, Path Patterns: /.*/videos/.*, /reel/.*, /places/..*/..*, /.*/posts/.*, /.*/photos/.*, /.*/photos, /.*/media_set, /.*/about, /.*/photos_of, /.*/photos_albums, /.*/friends, /inter_app/redirect/.*, /privacy_access_hub/.*, /contact_upload_settings/.*, /pg/.*/home, /pg/.*/home/, /pg/.*/about, /pg/.*/about/, /pg/.*/photos, /pg/.*/photos/, /pages/whatsapp, /pages, /fblite_transfer_your_information/.*, /dogfooding_assistant,

NETWORK SECURITY

HIGH: **4** | WARNING: **1** | INFO: **1** | SECURE: **2**

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.
4	*	high	Base config is configured to bypass certificate pinning.
5	facebook.com fbcdn.net fbsbx.com facebookcorewwwi.onion fbcdn23dssr3jqnq.onion fbsbx2q4mvcl63pw.onion instagram.com cdninstagram.com workplace.com oculus.com facebookvirtualassistant.com discoverapp.com freebasics.com internet.org viewpointsfromfacebook.com h.facebook.com l.facebook.com l.alpha.facebook.com lm.facebook.com l.instagram.com	secure	Domain config is securely configured to disallow clear text traffic to these domains in scope.

NO	SCOPE	SEVERITY	DESCRIPTION
6	facebook.com fbcdn.net fbsbx.com facebookcorewwwi.onion fbcdn23dssr3jqnq.onion fbsbx2q4mvcl63pw.onion instagram.com cdninstagram.com workplace.com oculus.com facebookvirtualassistant.com discoverapp.com freebasics.com internet.org viewpointsfromfacebook.com h.facebook.com l.facebook.com l.alpha.facebook.com lm.facebook.com l.instagram.com	info	Certificate pinning expires on 2024-10-03. After this date pinning will be disabled. [Pin: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4= Digest: SHA-256,Pin: ICGRfpgmOUXIWcQ/HXPLQTkFPEFPoDyjvH7ohhQpjzs= Digest: SHA-256,Pin: grX4Ta9HpZx6tSHkmCrvpApTQGo67CYDnvprLg5yRME= Digest: SHA-256,Pin: 58qRu/uxh4gFezqAcERupSkRYBlBAvfcw7mEjGPLnNU= Digest: SHA-256,Pin: r/mIkG3eEpVdm+u/ko/cwxzOMo1bk4TyHIlByibiA5E= Digest: SHA-256,Pin: i7WTqTvh0OioIruIfFR4kMPnBqrS2rdiVPl/s2uC/CY= Digest: SHA-256,Pin: uUwZgwDOxcBXrQcntwu+kYFpkiVkOaezL0WYEZ3anJc= Digest: SHA-256,Pin: WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18= Digest: SHA-256,Pin: Wd8xe/qfTwq3ylFNd3IpaqLHZbh2ZNCLluVzmeNkcpw= Digest: SHA-256,Pin: ape1HIIZ6T5d7GS61YBs3rD4NVvkfnVwELcCRW4Bqv0= Digest: SHA-256,Pin: oC+voZLIy4HLE0FVT5wFtxzKKokLDRKY1oNkfJYe+98= Digest: SHA-256,Pin: K87oWBWM9UZfyddvDfoxL+8lpNyoUB2ptGtn0fv6G2Q= Digest: SHA-256,Pin: cGuxAXyFXFkWm61cF4HPWX8S0srS9j0aSqN0k4AP+4A= Digest: SHA-256,Pin: aCdH+LpiG4fN07wpXtXKvOciocDANj0daLOJKNJ4fx4= Digest: SHA-256,Pin: rn+WLLnmp9v3uDP7GPqbcaiRdd+UnCMrap73yz3yu/w= Digest: SHA-256,Pin: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= Digest: SHA-256,Pin: diGVwiVYbubAI3RW4hB9xU8e/CH2GnkuvVFZE8zmgzI= Digest: SHA-256,Pin: q4PO2G2cbkZhZ82+JgmRUyGMoAeozA+BSXVXQWB8XWQ= Digest: SHA-256]
7	h.facebook.com l.facebook.com l.alpha.facebook.com lm.facebook.com l.instagram.com	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.
8	h.facebook.com l.facebook.com l.alpha.facebook.com lm.facebook.com l.instagram.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. []

CERTIFICATE ANALYSIS

HIGH: **1** | 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.
Certificate algorithm vulnerable to hash collision	high	Application is signed with MD5. MD5 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: **48** | WARNING: **7** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=15]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/fb_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	Launch Mode of activity (com.facebook.lite.MainActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
4	Broadcast Receiver (com.facebook.lite.pretos.LiteAppComponentReceiver) is not Protected. [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Broadcast Receiver (com.facebook.lite.rtc.IncomingCallReceiver) is not Protected. [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Broadcast Receiver (com.facebook.lite.campaign.CampaignReceiver) is not Protected. [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Broadcast Receiver (com.facebook.lite.appManager.AppManagerReceiver) is not Protected. [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Broadcast Receiver (com.facebook.lite.deviceid.FbLitePhoneIdRequestReceiver) is not Protected. [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Broadcast Receiver (com.facebook.appupdate.DownloadCompleteReceiver) is not Protected. [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Content Provider (com.facebook.lite.deviceid.FbLitePhoneIdProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Broadcast Receiver (com.facebook.lite.FbnsIntentService$CallbackReceiver) is not Protected. [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Broadcast Receiver (com.facebook.rti.push.service.MqttSystemBroadcastReceiver) is not Protected. [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Content Provider (com.facebook.lite.photo.MediaContentProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
14	Content Provider (com.facebook.lite.diode.UserValuesProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
15	Broadcast Receiver (com.facebook.lite.waotp.WAOtpCodeReceiver) is not Protected. [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
16	TaskAffinity is set for activity (com.facebook.lite.ShortcutActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
17	Activity (com.facebook.lite.ShortcutActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
18	TaskAffinity is set for activity (com.facebook.lite.rtc.RTCActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.

NO	ISSUE	SEVERITY	DESCRIPTION
19	Launch Mode of activity (com.facebook.lite.rtc.RTCActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
20	Launch Mode of activity (com.facebook.lite.webviewrtc.RTCIncomingCallActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
21	Launch Mode of activity (com.facebook.lite.nativeRtc.NativeRtcCallActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
22	Activity (com.facebook.lite.platform.LoginGDPDialogActivityV2) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
23	Activity (com.facebook.lite.waotp.WAOtpReceiveCodeActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
24	Activity-Alias (com.facebook.lite.deeplinking.activities.PermalinkPossiblePatternsActivityAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
25	Activity-Alias (com.facebook.lite.deeplinking.activities.PermalinkFBLinksAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
26	Activity-Alias (com.facebook.lite.deeplinking.UIQRE2EActivity) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
27	Activity-Alias (com.facebook.lite.deeplinking.activities.PermalinkLiteActivityAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
28	Activity-Alias (com.facebook.lite.stories.activities.ShareToFbStoriesAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
29	Activity-Alias (com.facebook.lite.stories.activities.ShareToFbMultiStoriesAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
30	Activity-Alias (com.facebook.lite.composer.activities.ShareIntentMultiPhotoAlphabeticalAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
31	Activity-Alias (com.facebook.lite.composer.activities.ShareIntentLinkGroupsAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
32	Activity-Alias (com.facebook.lite.composer.activities.ShareIntentMultiPhotoGroupsAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
33	Activity-Alias (com.facebook.lite.composer.activities.ShareIntentVideoGroupsAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
34	Activity-Alias (com.facebook.lite.composer.activities.ShareIntentVideoAlphabeticalAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
35	Activity-Alias (com.facebook.lite.composer.activities.ShareIntentMultiVideoAlphabeticalAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
36	Activity-Alias (com.facebook.lite.deeplinking.activities.PermalinkWatchShortAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
37	Activity-Alias (com.facebook.lite.deeplinking.activities.PermalinkFbliteMessagingFbMePrefixAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
38	Activity-Alias (com.facebook.lite.deeplinking.activities.CommunityChatsMDotMePrefixAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
39	Activity-Alias (com.facebook.lite.deeplinking.activities.PermalinkVanityPrefixAt) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
40	Activity-Alias (com.facebook.lite.deeplinking.activities.PermalinkVanityPrefixP) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
41	Activity-Alias (com.facebook.lite.deeplinking.activities.PermalinkVanityPrefixTilde) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
42	Activity-Alias (com.facebook.lite.deeplinking.activities.PermalinkHomeAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
43	Activity-Alias (com.facebook.lite.deeplinking.activities.PermalinkMessagingAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
44	Activity-Alias (com.facebook.lite.deeplinking.activities.PermalinkSettingsAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
45	Activity-Alias (com.facebook.lite.deeplinking.activities.PermalinkTimelineAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
46	Activity-Alias (com.facebook.lite.deeplinking.activities.PermalinkNotificationsAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
47	Activity-Alias (com.facebook.lite.deeplinking.activities.PermalinkProfileEditAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
48	Activity-Alias (com.facebook.lite.deeplinking.activities.PermalinkBuddylistAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
49	Activity-Alias (com.facebook.lite.deeplinking.activities.PermalinkExtraFacebookHostsAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
50	Activity-Alias (com.facebook.lite.composer.activities.ShareTextToMessagingAlias) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
51	Content Provider (com.facebook.lite.msys.LiteSecureMessagingKeyContentProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
52	Broadcast Receiver (com.facebook.oxygen.preloads.sdk.firstparty.managedappcache.IsManagedAppReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.facebook.appmanager.ACCESS [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
53	Service (com.facebook.secure.packagefinder.PackageFinderService) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
54	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
55	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
56	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/armeabi-v7a/libfb_xzdecoder.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/armeabi-v7a/libmemalign16.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/armeabi-v7a/libsuperpack-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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/armeabi-v7a/libsigmux.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/armeabi-v7a/libbreakpad_cpp_helper.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	lib/armeabi-v7a/libc++_shared.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/x86/libfb_xzdecoder.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	lib/x86/libmemalign16.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	lib/x86/libsuperpack-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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	lib/x86/libsigmux.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	lib/x86/libbreakpad_cpp_helper.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	lib/x86/libc++_shared.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	lib/armeabi-v7a/libfb_xzdecoder.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	lib/armeabi-v7a/libmemalign16.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	lib/armeabi-v7a/libsuperpack-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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	lib/armeabi-v7a/libsigmux.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	lib/armeabi-v7a/libbreakpad_cpp_helper.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	lib/armeabi-v7a/libc++_shared.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	lib/x86/libfb_xzdecoder.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	lib/x86/libmemalign16.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	lib/x86/libsuperpack-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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	lib/x86/libsigmux.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	lib/x86/libbreakpad_cpp_helper.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.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	lib/x86/libc++_shared.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.	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.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

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.facebook.com	ok	**IP:** 157.240.205.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
m.facebook.com	ok	**IP:** 157.240.205.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyBWJZPw7wVi-NQEViQV9ZnadO-xbX4S8o0"

PLAYSTORE INFORMATION

Title: Facebook Lite

Score: 3.5480988 **Installs:** 1,000,000,000+ **Price:** 0 **Android Version Support:** **Category:** Social **Play Store URL:** com.facebook.lite

Developer Details: Meta Platforms, Inc., Meta+Platforms,+Inc., 1 Hacker Way Menlo Park, CA 94025, https://www.facebook.com/facebook, lite-android-support@fb.com,

Release Date: Mar 15, 2018 **Privacy Policy:** Privacy link

Description:

Keeping up with friends is faster and easier than ever with the Facebook Lite app! Use Facebook Lite as a friends app to connect and keep up with your social network. The Facebook Lite app is small, allowing you to save space on your phone and use Facebook in 2G conditions. Many of the classic features of Facebook are available on the app, such as sharing to a Timeline, liking photos, searching for people, and editing your profile and groups. Specific features include: • Find friends and family • Post status updates & use Facebook emoji to help relay what’s going on in your world • Share photos and your favorite memes • Get notified when friends like and comment on your posts • Find local social events, RSVP, and make plans to meet up with friends • Interact with your friends by adding your own comments or reactions to their Facebook posts • Save photos by adding them to photo albums • Follow people to get their latest news • Look up local businesses to see reviews, operation hours, and pictures • Buy and sell locally on Facebook Marketplace The Facebook app does more than help you stay connected with your friends and interests. It's also your personal organizer for storing, saving and sharing photos. It's easy to share photos straight from your Android camera, and you have full control over your photos and privacy settings. You can choose when to keep individual photos private or even set up a secret photo album to control who sees it. Facebook Lite also helps you keep up with the latest news and current events around the world. Subscribe to your favorite celebrities, brands, websites, artists, or sports teams to follow their News Feeds from the convenience of your Facebook Lite app! Problems with downloading or installing the app? See https://www.facebook.com/help/fblite Still need help? Please tell us more about the issue: https://www.facebook.com/help/contact/640732869364975 Facebook is only available to people aged 13 and over. Terms of Service: http://m.facebook.com/terms.php

---

Report Generated by - MobSF v3.7.9 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.