MOBSF

ANDROID STATIC ANALYSIS REPORT

InstaPro (240.2.0.18.107)

File Name:	InstaPro_240.2.0.18.107_apkcombo.com.apk
Package Name:	com.instapro.android
Scan Date:	Aug. 18, 2022, 12:14 p.m.
App Security Score:	23/100 (CRITICAL RISK)
Grade:	
Trackers Detection:	2/428

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
59	37	3	4	1

FILE INFORMATION

File Name: InstaPro_240.2.0.18.107_apkcombo.com.apk
Size: 55.54MB
MD5: 38d3baa0f2a2dd36883dd28c948c20c5
SHA1: 0f92a0929c0dd283862b19f54e6a74b7c54ac9f5
SHA256: 2005fd77664eb4dfc0faa6f17fed2176d0fda9c8e78f65b970bc31dc64fee9f2

APP INFORMATION

App Name: InstaPro ♚
Package Name: com.instapro.android
Main Activity: com.instagram.settings.activity.NotificationSettingsHandlerActivity
Target SDK: 29
Min SDK: 21
Max SDK:
Android Version Name: 240.2.0.18.107

Android Version Code: 364004862

APP COMPONENTS

Activities: 209
Services: 77
Receivers: 43
Providers: 11
Exported Activities: 29
Exported Services: 12
Exported Receivers: 15
Exported Providers: 8

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2008-02-29 01:33:46+00:00
Valid To: 2035-07-17 01:33:46+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
Serial Number: 0x936eacbe07f201df
Hash Algorithm: sha1
md5: e89b158e4bcf988ebd09eb83f5378e87
sha1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
sha256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
sha512: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	high	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 SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.USE_FULL_SCREEN_INTENT	normal		Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_MEDIA_LOCATION	dangerous	access any geographic locations	Allows an application to access any geographic locations persisted in the user's shared collection.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.instagram.direct.permission.PROTECTED_DEEPLINKING	unknown	Unknown permission	Unknown permission from android reference
com.instagram.direct.permission.DIRECT_APP_THREAD_STORE_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.facebook.services.identity.FEO2	unknown	Unknown permission	Unknown permission from android reference
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.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.sonyericsson.home.permission.BROADCAST_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
.permission.RECEIVE_ADM_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.amazon.device.messaging.permission.RECEIVE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference
android.permission.MANAGE_OWN_CALLS	normal		Allows a calling application which manages it own calls through the self-managed ConnectionService APIs.
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.
com.instapro.android.permission.CROSS_PROCESS_BROADCAST_MANAGER	unknown	Unknown permission	Unknown permission from android reference
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_BIOMETRIC	normal		Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti Disassembly Code — DETAILS: illegal class name FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check FINDINGS: Compiler — DETAILS: dexlib 2.x

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
SIM operator check
network operator name check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes6.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>classes7.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.HARDWARE check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>classes8.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.instagram.android.activity.MainTabActivity	Schemes: instagram://, Hosts: headline_event, story-camera, live_camera, reels-camera, direct-inbox, share, reels_home, news, mainfeed,
com.facebook.secure.deeplink.GlobalUriHandlerActivity	Schemes: instagram://, Hosts: ecp_checkout,

ACTIVITY	INTENT
com.instagram.url.UrlHandlerLauncherActivity	Schemes: http://, https://, instagram://, Hosts: instagram.com, www.instagram.com, applink.instagram.com, familycenter.instagram.com, call.instagram.com, ig.me, active_promotions, ads_payments_prepay_payment_status, android, approved_accounts, business_sign_up, business_profile_calling, call_settings, branded_content, branded_content_deal_creator_payout, branded_content_project, branded_content_ad, shops_directory, community_content, cowatch, create_room, create_post, suggested_reply, quick_replies, explore, enter_promotion_payment, editprofile, edit_profile_bio, fundraiser, guide, media, acredirect, inter_app/redirect, open_access_application_enrollment, stories, open_access_profile_review_status, product_display_page, professional_sign_up, promote, professional_onboarding_checklist, professional_dashboard, profile, profile_shop, tag, user, fb_friends, fbpay_hub, bizwallet, bloks_native_hybrid_shell, shopping_seller_management_creator_media, products_for_you, reconsideration_products_for_you, firestarter_buyer_bootstrap, recommendations_in_explore_products, payments, shop_pay_did_finish, update_payment, bloks_order_receipt, hub_order_details, orders_hub, business_order, follow_and_invite_friends, ig_payout_hub, ad_topics, insights, tv, igtv_profile, shopping_editorial, settings_payments, settings_theme, settings, ads_pay_now, fbe_app_store, ad_activity, ads_payments, fxim_name_changing_reminder, account_link_auth, smb_select_partner, smb_purchase_options, smb_edit_partner, smsrecovery, voting_info_center, create_shopping_tagged_post, shop_manager_add_products, shop_manager_edit_products, shopping_home, seller_screen_delegator, igtv_revshare_onboarding, user_pay_onboarding, subscriptions_management, affiliate_management, affiliate_checklist, affiliate_activate_bonus, affiliate_partnership_discovery_opt_in, incentive_platform_management, incentive_platform_available_bonus, incentive_platform_progress_tracking, resume_payout_onboarding, product_eligibility, igtv_upload, product_composer, product_collection, open_xac, reels, reels_share, reels_effect_page, audio, audio_page, business_spa_hub, calendar_auth_success, calendar_auth_failure, calendar_auth_launch, discounts_interstitial, thread, seller_actions_bloks_app, creator_monetization_contact_support, creator_settings, direct-thread, direct_message_options, shopping_guidance_router, technical_incident, bloks_leave_review, view_lead_details, aradscamera, ar_commerce, upload_contacts_settings, extbrowser, ar, embeds_opt_out_setting, avatar_sticker_upsell_bloks_action, map, shopping_creator_shop_management, injected_feed_unit_products, discovery_home, messaging_hub, tyi/mobile, collection, manage_qa_private_reply, survey, virtual_object,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.instagram.android,

NETWORK SECURITY

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 2023-07-1. After this date pinning will be disabled. [Pin: lCppFqbkrlJ3EcVFAkeip0+44VaoJUymbnOaEUk7tEU= Digest: SHA-256,Pin: grX4Ta9HpZx6tSHkmCrvpApTQGo67CYDnvprLg5yRME= Digest: SHA-256,Pin: l/Lt/z7ekCWanjD0Cvj5EqXls2lOaThEA0H2Bg4BT/o= Digest: SHA-256,Pin: 8ca6Zwz8iOTfUpc8rkIPCgid1HQUT+WAbEIAZOFZEik= Digest: SHA-256,Pin: Fe7TOVlLME+M+Ee0dzcdjW/sYfTbKwGvWJ58U7Ncrkw= 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: PZXN3lRAy+8tBKk2Ox6F7jIlnzr2Yzmwqc3JnyfXoCw= Digest: SHA-256,Pin: WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18= Digest: SHA-256,Pin: Wd8xe/qfTwq3ylFNd3IpaqLHZbh2ZNCLluVzmeNkcpw= Digest: SHA-256,Pin: K87oWBWM9UZfyddvDfoxL+8lpNyoUB2ptGtn0fv6G2Q= Digest: SHA-256,Pin: iie1VXtL7HzAMF+/PVPR9xzT80kQxdZeJ+zduCB3uj0= Digest: SHA-256,Pin: cGuxAXyFXFkWm61cF4HPWX8S0srS9j0aSqN0k4AP+4A= 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. []

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag 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.
3	Activity (com.OM7753.gold.PinLockActivity) 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
4	Activity (com.instagram.mainactivity.LauncherActivity) 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.
5	Activity (com.instagram.mainactivity.MainActivity) 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.
6	Activity-Alias (com.instagram.android.activity.MainTabActivity) 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.
7	Activity (com.instagram.url.UrlHandlerActivity) 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
8	Activity (com.instagram.url.UrlHandlerLauncherActivity) 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.
9	Activity (com.facebook.CustomTabActivity) 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
10	Service (com.facebook.fbreact.autoupdater.ighttp.IgHttpUpdateGcmTaskService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
11	Service (com.facebook.rti.push.service.FbnsService) 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
12	Content Provider (com.instagram.contentprovider.users.impl.IgLoggedInUsersContentProvider) 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.
13	Broadcast Receiver (com.instagram.launcherbadges.LauncherBadgesReceiver) 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
14	Service (com.instagram.util.offline.BackgroundPrefetchGcmTaskService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
15	Content Provider (com.instagram.contentprovider.CurrentUserProvider) 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
16	Content Provider (com.instagram.contentprovider.FamilyAppsUserValuesProvider) 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.
17	Content Provider (com.instagram.common.analytics.fdidlite.InstagramFDIDLiteProvider) 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.
18	Content Provider (com.instagram.direct.notifications.contentprovider.AppBackgroundStateContentProvider) 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.
19	Content Provider (com.instagram.direct.notifications.filters.contentprovider.DirectShouldDisplayNotificationFilterContentProvider) 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
20	Service (com.instagram.direct.stella.StellaDirectMessagingService) 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.
21	Activity (com.instagram.direct.stella.permission.StellaPermissionActivity) 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.
22	Content Provider (com.instagram.realtimeclient.ipc.contentprovider.RealtimeClientKeepAliveContentProvider) 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.
23	Broadcast Receiver (com.instagram.notifications.push.fbns.FbnsPushNotificationHandler$IgFbnsCallbackReceiver) 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
24	Broadcast Receiver (com.instagram.common.analytics.phoneid.InstagramPhoneIdRequestReceiver) 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.
25	Content Provider (com.instagram.common.analytics.phoneid.InstagramPhoneIdProvider) 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.
26	Broadcast Receiver (com.instagram.pendingmedia.service.impl.ConnectivityChangeReceiver) 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.
27	Broadcast Receiver (com.instagram.appcomponentmanager.IgAppComponentReceiver) 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
28	Broadcast Receiver (com.instagram.notifications.push.ADMMessageHandler$Receiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.amazon.device.messaging.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.

NO	ISSUE	SEVERITY	DESCRIPTION
29	TaskAffinity is set for Activity (com.instagram.share.handleractivity.ShareHandlerActivity)	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.
30	Activity (com.instagram.share.handleractivity.ShareHandlerActivity) 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
31	TaskAffinity is set for Activity (com.instagram.share.handleractivity.StoryShareHandlerActivity)	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.
32	Activity (com.instagram.share.handleractivity.StoryShareHandlerActivity) 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
33	TaskAffinity is set for Activity (com.instagram.share.handleractivity.ReelShareHandlerActivity)	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.
34	Activity (com.instagram.share.handleractivity.ReelShareHandlerActivity) 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
35	TaskAffinity is set for Activity (com.instagram.share.handleractivity.MultiStoryShareHandlerActivity)	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.
36	Activity (com.instagram.share.handleractivity.MultiStoryShareHandlerActivity) 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
37	TaskAffinity is set for Activity (com.instagram.share.handleractivity.CustomStoryShareHandlerActivity)	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.
38	Activity (com.instagram.share.handleractivity.CustomStoryShareHandlerActivity) 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
39	TaskAffinity is set for Activity (com.instagram.share.handleractivity.ClipsShareHandlerActivity)	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.
40	Activity (com.instagram.share.handleractivity.ClipsShareHandlerActivity) 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
41	TaskAffinity is set for Activity (com.instagram.modal.TransparentOutOfAppPictureInPictureModalActivity)	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.
42	TaskAffinity is set for Activity (com.instagram.modal.IGTVPictureInPictureModalActivity)	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
43	Broadcast Receiver (com.instagram.push.InstagramAppUpgradeEventReceiver) 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.
44	Broadcast Receiver (com.instagram.push.FbnsInitBroadcastReceiver) 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
45	Service (com.facebook.analytics2.logger.GooglePlayUploadService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
46	Broadcast Receiver (com.instagram.publisher.CopypastaConnectivityChangeReceiver) 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
47	Broadcast Receiver (com.facebook.appcomponentmanager.testreceivers.AppComponentManagerTestingReceiver) 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.
48	Broadcast Receiver (com.facebook.appcomponentmanager.testreceivers.FirstEnableStageTestReceiver) 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.
49	Broadcast Receiver (com.facebook.appcomponentmanager.testreceivers.SecondEnableStageTestReceiver) 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
50	Service (com.facebook.common.errorreporting.memory.service.jobschedulercompat.DumperUploadGcmTaskService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
51	Service (com.instagram.notifications.push.fcm.IgFirebaseMessagingService) 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
52	Service (com.instagram.notifications.push.fcm.GetFCMTokenAndRegisterWithServerGCMService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
53	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.

NO	ISSUE	SEVERITY	DESCRIPTION
54	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
55	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [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.

NO	ISSUE	SEVERITY	DESCRIPTION
56	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.
57	Activity (com.instagram.platform.AppAuthorizeActivity) 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
58	TaskAffinity is set for Activity (com.instagram.direct.share.handler.DirectShareHandlerActivity)	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.
59	Activity (com.instagram.direct.share.handler.DirectShareHandlerActivity) 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.
60	Activity-Alias (com.instagram.direct.share.handler.DirectShareHandlerActivityInterop) 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
61	TaskAffinity is set for Activity (com.instagram.direct.share.handler.DirectExternalMediaShareActivity)	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.
62	Activity (com.instagram.direct.share.handler.DirectExternalMediaShareActivity) 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.
63	Activity-Alias (com.instagram.direct.share.handler.DirectExternalMediaShareActivityPhoto) 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
64	Activity-Alias (com.instagram.direct.share.handler.DirectExternalMediaShareActivityPhotoInterop) 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.
65	Activity-Alias (com.instagram.direct.share.handler.DirectExternalMediaShareActivityVideo) 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.
66	Activity-Alias (com.instagram.direct.share.handler.DirectExternalMediaShareActivityVideoInterop) 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.
67	Activity (com.instagram.direct.share.handler.DirectMultipleExternalMediaShareActivity) 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
68	Activity-Alias (com.instagram.direct.share.handler.DirectMultipleExternalMediaShareActivityInterop) 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.
69	Service (com.instagram.direct.share.choosertarget.DirectChooserTargetService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_CHOOSER_TARGET_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
70	TaskAffinity is set for Activity (com.instagram.rtc.activity.RtcCallActivity)	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.
71	TaskAffinity is set for Activity (com.instagram.rtc.activity.RtcCallIntentHandlerActivity)	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
72	Activity (com.instagram.fbpay.w3c.views.PaymentActivity) 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.
73	Service (com.instagram.fbpay.w3c.ipc.IsReadyToPayServiceImpl) 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.
74	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
75	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) 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
76	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) 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.
77	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.

NO	ISSUE	SEVERITY	DESCRIPTION
78	Activity-Alias (com.facebook.secure.packagefinder.PackageFinderActivity) 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.
79	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
				X/AbstractC013805y.java X/AbstractC09400eS.java X/AbstractC14280nw.java X/AbstractC1571873a.java X/AbstractC162347Pm.java X/AbstractC230419z.java X/AbstractC23151An.java X/AbstractC36791Gdd.java X/AbstractC38657Hcx.java X/AbstractC40023IFk.java X/AbstractC41282Ixk.java X/AbstractC41286Ixp.java X/AbstractC50382Zg.java X/AbstractC54322gN.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				X/AbstractC5452gN.java X/AbstractDialogInterface$OnCancelListener C41236Iwc.java X/AbstractDialogInterface$OnClickListenerC 73413bV.java X/AbstractRunnableC38041qe.java X/AbstractServiceC021009f.java X/AbstractServiceC39355Htk.java X/AnonymousClass029.java X/AnonymousClass033.java X/AnonymousClass156.java X/AnonymousClass229.java X/AnonymousClass340.java X/AnonymousClass355.java X/AnonymousClass868.java X/C00N.java X/C00Q.java X/C01G.java X/C01b.java X/C02280Af.java X/C02R.java X/C03120Dr.java X/C03200Dz.java X/C03630Jg.java X/C03660Jn.java X/C03670Jo.java X/C03850Km.java X/C03920Ky.java X/C05Y.java X/C07850bF.java X/C07900bK.java X/C07920bM.java X/C08090be.java X/C08370cB.java X/C09270eC.java X/C09340eJ.java X/C09410eT.java X/C09880fF.java X/C0AX.java X/C0E9.java X/C0EW.java X/C0FF.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				X/C0FE.java X/C0FN.java X/C0FQ.java X/C0GP.java X/C0J4.java X/C0JD.java X/C0Jj.java X/C0K1.java X/C0KS.java X/C0KV.java X/C0L8.java X/C0LC.java X/C0TB.java X/C0TC.java X/C0U8.java X/C0VD.java X/C0YH.java X/C101184j1.java X/C102794lp.java X/C11420it.java X/C11460iy.java X/C11540j7.java X/C118175Ua.java X/C119015Yf.java X/C119055Yj.java X/C12090kF.java X/C14270nv.java X/C144726eZ.java X/C144736ea.java X/C144746eb.java X/C144756ec.java X/C144776ee.java X/C144796eg.java X/C14690oj.java X/C15000pE.java X/C15220pe.java X/C15230pf.java X/C159887Es.java X/C16650sN.java X/C16710sU.java X/C170277kM.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				X/C170287kN.java X/C170327kR.java X/C171057lc.java X/C171157lm.java X/C18890wP.java X/C18L.java X/C18Z.java X/C1B2.java X/C1B9.java X/C1C9.java X/C1UB.java X/C1UC.java X/C1UK.java X/C1r7.java X/C226418h.java X/C22C.java X/C29321aJ.java X/C29451ac.java X/C29541am.java X/C29701b5.java X/C29831bK.java X/C29911bU.java X/C2B5.java X/C2BE.java X/C2BG.java X/C2QE.java X/C2SI.java X/C2UH.java X/C2r6.java X/C30041bh.java X/C30151bs.java X/C30281c6.java X/C30301c8.java X/C31G.java X/C32A.java X/C32e.java X/C34663Fb0.java X/C34770Fd5.java X/C34772Fd9.java X/C34F.java X/C35E.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				X/C35P.java X/C357.java X/C36499GUq.java X/C36816Ge4.java X/C36864Gev.java X/C36Q.java X/C37058Gjf.java X/C37157GlU.java X/C37266Gna.java X/C37393Gq1.java X/C37524GsQ.java X/C37592Gtk.java X/C37617GuF.java X/C37845GyB.java X/C38199HEl.java X/C38321rC.java X/C38422HTl.java X/C38482HXa.java X/C38512HZp.java X/C38536HaJ.java X/C38574Hb8.java X/C38633HcQ.java X/C38718He8.java X/C38820Hg7.java X/C38A.java X/C39046HoY.java X/C39281su.java X/C39291sv.java X/C39321sy.java X/C39335HtQ.java X/C39352Hth.java X/C39357Htn.java X/C39359Htp.java X/C39361Htr.java X/C39367Hu1.java X/C39385HuN.java X/C39443HvO.java X/C39588HyA.java X/C39599HyM.java X/C39608Hya.java X/C39609Hyb.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	X/C39636Hz6.java X/C39638HzF.java X/C39649Hza.java X/C39650Hzb.java X/C39752I3o.java X/C39755I3s.java X/C3Qk.java X/C3X7.java X/C3XI.java X/C3Y6.java X/C40395Iay.java X/C40666Igt.java X/C40931Inn.java X/C41201Iv0.java X/C41216Ivl.java X/C41262IxM.java X/C41263IxN.java X/C41268IxT.java X/C41269IxU.java X/C41288Ixr.java X/C41299Iy4.java X/C41301Iy6.java X/C41319IyO.java X/C41323IyT.java X/C41385IzZ.java X/C42080JbB.java X/C42106Jbg.java X/C42377JgO.java X/C42385JgX.java X/C42386JgY.java X/C42593JkQ.java X/C42594JkR.java X/C42595JkS.java X/C427121u.java X/C43690KWm.java X/C43760KZg.java X/C44682Ap.java X/C49R.java X/C4C5.java X/C4WY.java X/C51I.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				X/C53812fX.java X/C54022fs.java X/C54512gg.java X/C57682mC.java X/C57732mI.java X/C59Y.java X/C5MD.java X/C5Uf.java X/C64162zK.java X/C649532c.java X/C651132w.java X/C656134y.java X/C658335v.java X/C68513Hv.java X/C68543Hy.java X/C68953Kd.java X/C69003Ki.java X/C70433Ql.java X/C71893Xd.java X/C72883ab.java X/C73423bW.java X/C79593mo.java X/C7JK.java X/C85093wM.java X/C8F0.java X/C93394Px.java X/C98794f2.java X/CallableC155606yR.java X/CallableC42388Jga.java X/GXE.java X/GXW.java X/GYI.java X/H2O.java X/H5C.java X/H5J.java X/HHK.java X/HS0.java X/HS1.java X/HU4.java X/HandlerC38916Hm2.java X/HandlerC39651Hzc.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				X/HandlerC41292Ixv.java X/HandlerC41322IyS.java X/HandlerThreadC68233Gs.java X/HuH.java X/HuK.java X/I13.java X/I14.java X/I3Q.java X/ICJ.java X/IMW.java X/J2K.java X/K4Z.java X/K8T.java X/K8X.java X/K8Z.java X/K8b.java X/K8f.java X/K8h.java X/K8j.java X/K8k.java X/K8l.java X/K8o.java X/RunnableC36790Gdc.java X/RunnableC37433Gqi.java X/RunnableC39360Htq.java X/RunnableC39369Hu3.java X/RunnableC39380HuF.java X/RunnableC41162It3.java X/RunnableC41273IxY.java X/RunnableC41320IyP.java X/RunnableC42404Jgr.java X/RunnableC53352ej.java X/ServiceConnectionC39370Hu4.java X/ServiceConnectionC39753I3p.java X/ServiceConnectionC41285Ixo.java X/ServiceConnectionC42393Jgf.java X/ServiceConnectionC73053as.java X/TextureView$SurfaceTextureListenerC102734lj.java X/View$OnAttachStateChangeListenerC37013Gih.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				X/View$OnClickListenerC38393HRy.java X/View$OnKeyListenerC41467J3w.java X/View$OnKeyListenerC48112Ou.java com/OM7753/acra/CrashReportDialog.java com/OM7753/acra/CrashReportFinder.java com/OM7753/acra/ErrorReporter.java com/OM7753/acra/SendWorker.java com/OM7753/acra/collector/ConfigurationCollector.java com/OM7753/acra/collector/CrashReportDataFactory.java com/OM7753/acra/collector/DeviceFeaturesCollector.java com/OM7753/acra/collector/DropBoxCollector.java com/OM7753/acra/collector/DumpSysCollector.java com/OM7753/acra/collector/LogCatCollector.java com/OM7753/acra/collector/SettingsCollector.java com/OM7753/acra/log/AndroidLogDelegate.java com/OM7753/acra/sender/GoogleFormSender.java com/OM7753/acra/sender/HttpSender.java com/OM7753/acra/util/Installation.java com/OM7753/acra/util/PackageManagerWrapper.java com/OM7753/acra/util/ReportUtils.java com/OM7753/acra/util/ToastSender.java com/OM7753/gold/EnhancedMovementMethod.java com/OM7753/gold/GOLD.java com/OM7753/gold/ImageActivity.java com/OM7753/gold/ImageViewer.java com/OM7753/gold/Live.java com/OM7753/gold/PermissionDialog.java com/OM7753/gold/backup/PrefsBackupHelper.java com/color/ColorSelectorDialog.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/color/HexSelectorView.java com/dolby/voice/devicemanagement/common/OsAudioManagerHelperBase.java com/dolby/voice/devicemanagement/common/OsAudioManagerHelperPreApi23.java com/dolby/voice/devicemanagement/common/OsBluetoothHelper.java com/dolby/voice/devicemanagement/common/OsBluetoothHelperBase.java com/dolby/voice/devicemanagement/common/OsBluetoothHelperPreApi23.java com/dolby/voice/devicemanagement/common/OsUsbHelper.java com/dolby/voice/devicemanagement/devices/AudioDevicesManagerAboveApi31.java com/dolby/voice/devicemanagement/devices/AudioDevicesManagerBase.java com/dolby/voice/devicemanagement/mode/AudioModeManager.java com/dolby/voice/devicemanagement/utils/Task.java com/file/firzen/mukkiasevaigal/M.java com/hippo/unifile/DocumentsContractApi19.java com/hippo/unifile/DocumentsContractApi21.java com/hippo/unifile/RawFile.java com/hippo/unifile/TreeDocumentFile.java com/hippo/unifile/TrickRandomAccessFile.java com/instagram/arlink/ui/GridPatternView.java com/instagram/common/gallery/Medium.java com/instagram/debug/logdelegate/IgLogImpl.java com/instagram/nux/activity/SignedOutFragmentActivity.java com/instagram/realtimeclient/RealtimeClientManager.java com/instagram/realtimeclient/fleetbeacon/F

NO	ISSUE	SEVERITY	STANDARDS	FILES
				leetBeaconRealtimeReceivePublishEventHandler.java com/users/Dll.java exoplayer2/av1/src/Dav1dDecoder.java org/microg/safeparcel/AutoSafeParcelable.java org/slf4j/LoggerFactory.java
				X/AbstractC30101bn.java X/AbstractC35791mi.java X/AnonymousClass323.java X/C001300l.java X/C001400m.java X/C003901p.java X/C00Q.java X/C021309i.java X/C021409k.java X/C02Z.java X/C03C.java X/C06800Yq.java X/C06850Yv.java X/C09j.java X/C0AC.java X/C0JM.java X/C0KX.java X/C0P2.java X/C0QG.java X/C0QY.java X/C0U8.java X/C0UA.java X/C0ZN.java X/C0ZR.java X/C11540j7.java X/C12M.java X/C13330mL.java X/C13550mi.java X/C13S.java X/C13Y.java X/C149276mY.java X/C149336me.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	X/C163747Vt.java X/C163807Vz.java X/C1GU.java X/C1WJ.java X/C1WN.java X/C1X2.java X/C222416p.java X/C24071Ew.java X/C24I.java X/C28091Wa.java X/C28H.java X/C30251c3.java X/C31141e9.java X/C33141iB.java X/C33271iP.java X/C34546FXr.java X/C35231lg.java X/C35761mf.java X/C35771mg.java X/C36399GPt.java X/C3HY.java X/C3OD.java X/C41229IwD.java X/C4FP.java X/C54302gL.java X/C55342i6.java X/C63702yG.java X/C63732yJ.java X/C67903Fa.java X/C76463gr.java X/C7C5.java X/C86273yR.java X/C883644t.java X/C89614Ap.java X/FXC.java X/GE8.java X/HWH.java X/IA4.java X/KDR.java X/KS2.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				X/KS4.java X/KS5.java X/KS8.java com/instagram/debug/network/NetworkShapingRequestCallback.java com/instagram/realtimeclient/RealtimeClientConfig.java com/instagram/realtimeclient/RealtimeClientManager.java com/instagram/realtimeclient/requeststream/SubscribeExecutor.java com/instagram/ui/widget/balloonsview/BalloonsView.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	X/C0NY.java X/C18680vu.java X/C1UY.java X/C29451ac.java X/C36884GfH.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	X/C06630Xy.java X/C0L0.java X/C0Q6.java X/C11F.java X/C15300pu.java X/C18840wK.java X/C1SO.java X/C27521Tr.java X/C29351aM.java X/C34661kk.java X/C36973Ghv.java X/C38574Hb8.java X/C39541tP.java X/C5MR.java X/C84s.java X/EnumC44372Kog.java X/HSO.java X/HST.java X/HZV.java X/I0Q.java X/View$OnClickListenerC1800984p.java com/OM7753/gold/DownloadFragment.java com/OM7753/gold/GOLD.java com/OM7753/gold/backup/PrefsBackupHelper.java com/file/firzen/filelister/FileListerAdapter.java com/hippo/unifile/DocumentsContractApi19.java com/instagram/pendingmedia/store/PendingMediaStore.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	X/A0BX.java X/C1Dq.java X/C23471Bz.java X/C38663Hd9.java X/C38664HdA.java X/C4GM.java X/C85513x2.java
6	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	X/C005302e.java X/C167947fu.java X/C16890sm.java X/C38365HQh.java X/C38599HbY.java X/C39596HyJ.java X/C39668Hzt.java X/I0G.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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	X/AnonymousClass793.java X/C06630Xy.java X/C0SN.java X/C11460iy.java X/C115645Im.java X/C119015Yf.java X/C119235Zb.java X/C1573673t.java X/C167947fu.java X/C1E0.java X/C1NS.java X/C23691De.java X/C27441Tj.java X/C66853Ac.java X/C74443dN.java X/C74D.java X/C80773p9.java X/CallableC168677hF.java X/EnumC58642oJ.java X/HSP.java X/RunnableC1576175b.java
8	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	X/C9XM.java X/JMY.java com/file/firzen/mukkiasevaigal/S.java com/instagram/base/activity/IgFragmentActivity.java com/instagram/direct/msys/armadillo/IGSecureMessageMasterKeyProvider.java com/instagram/react/modules/product/IgReactPurchaseExperienceBridgeModule.java com/instagram/react/views/maps/IgStaticMapViewManager.java com/instagram/realtimeclient/PresenceSubscriptionIDStore.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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	X/C0XI.java X/C197768tR.java X/C26521Bs3.java X/MenuItem$OnMenuItemClickListenerC38327HOa.java com/OM7753/gold/GOLD.java com/OM7753/gold/OnDonateClick.java com/OM7753/gold/TranslateCopyClick.java com/instagram/debug/devoptions/debugheap/data/provider/LoomTraceHelper.java
10	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	X/C0L5.java X/C0v5.java X/C160077Fn.java X/C16710sU.java X/C38429HTv.java X/C38599HbY.java X/C39081sY.java X/C39595HyI.java X/C40907Imx.java X/C66853Ac.java X/C82653sH.java
11	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	X/C03930Kz.java X/C0T2.java X/C14C.java X/C216113d.java X/I2W.java X/I2X.java
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	X/C1SO.java X/C1UB.java X/HZR.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
13	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	X/FQU.java X/HTr.java
14	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	X/ICJ.java com/instagram/direct/msys/armadillo/IGSecureMessageCryptoProvider.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/armeabi-v7a/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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/armeabi-v7a/libfb_xzdecoder.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/armeabi-v7a/libfbjni.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/armeabi-v7a/libbreakpad.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/armeabi-v7a/libfbgloginit.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	lib/armeabi-v7a/libsigmux.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/armeabi-v7a/libandroid_aware_dlopen.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	lib/armeabi-v7a/libglog.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	lib/armeabi-v7a/libwatcher_binary.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	lib/armeabi-v7a/liblinkerutils.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	lib/armeabi-v7a/libmemalign16.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	lib/armeabi-v7a/libunwindstack_binary.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.	$ORIGIN/unwindstack_binary-binary#android-armv7,binary,shared-library-symlink-tree high The shared object has RUNPATH set. In certain cases an attacker can abuse this feature and or modify environment variables to run arbitrary shared objects for code execution and privilege escalation. The only time a shared library in should set RUNPATH is if it is linked to private shared libraries in the same package. Remove the compiler option --enable-new-dtags,-rpath to remove RUNPATH.	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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	lib/armeabi-v7a/libbreakpad_cpp_helper.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	lib/armeabi-v7a/libsuperpack-jni.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	lib/armeabi-v7a/liblmkd_detector_binary.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	lib/armeabi-v7a/libdistract.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	lib/armeabi-v7a/libelf.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	lib/armeabi-v7a/libfb.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	lib/armeabi-v7a/libzstddecoder.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	lib/armeabi-v7a/libfacebook-core.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	lib/armeabi-v7a/libarcore_sdk_jni.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.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	lib/armeabi-v7a/libforce_dlopen.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.

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 ['bluetooth', 'camera', 'microphone', 'network connectivity', 'location'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to ['address book'].
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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.
12	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit.
13	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.
14	FCS_COP.1.1(3)	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
15	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'] .

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
16	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
17	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
18	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.
19	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The certificate path must terminate with a trusted CA certificate'].
20	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.
21	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.
22	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
sammods.link	ok	**IP:** 207.174.213.150 **Country:** United States of America **Region:** Massachusetts **City:** Burlington **Latitude:** 42.508480 **Longitude:** -71.201134 **View:** Google Map
www.bloks.commerce.creator-shop.activation.info	ok	**IP:** 64.190.63.111 **Country:** Germany **Region:** Nordrhein-Westfalen **City:** Koeln **Latitude:** 50.933331 **Longitude:** 6.950000 **View:** Google Map
www.avatar.editor.cds.launcher	ok	No Geolocation information available.
i.imgur.com	ok	**IP:** 199.232.148.193 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
translate.googleapis.com	ok	**IP:** 173.194.222.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.minishops.ssh.data	ok	No Geolocation information available.
z-m-portal.fb.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
v.whatsapp.net	ok	**IP:** 157.240.205.60 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
scontent-lhr8-1.xx.fbcdn.net	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
checkout.us.shopifycs.com	ok	**IP:** 35.223.179.95 **Country:** United States of America **Region:** Iowa **City:** Council Bluffs **Latitude:** 41.261940 **Longitude:** -95.860832 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sammods.github.io	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
maps.google.com	ok	**IP:** 64.233.162.138 **Country:** Brazil **Region:** Sao Paulo **City:** Sao Paulo **Latitude:** -23.547501 **Longitude:** -46.636108 **View:** Google Map
www.fxim.sync.interop.async	ok	No Geolocation information available.
maps.googleapis.com	ok	**IP:** 74.125.131.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.ig.pro	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.prod.facebook.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
www.bloks.commerce.creators-as-sellers.manage-partner-permission	ok	No Geolocation information available.
www.instamod.net	ok	**IP:** 74.125.131.121 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
business.facebook.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
www.xstack	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
graph.facebook.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
www.bloks.commerce.checkout.update	ok	No Geolocation information available.
expresswifi.com	ok	No Geolocation information available.
www.instapro	ok	No Geolocation information available.
maps.instagram.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
softwareengineering.stackexchange.com	ok	**IP:** 151.101.193.69 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
help.instagram.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
web.facebook.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
www.messenger.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
bit.ly	ok	**IP:** 67.199.248.10 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
www.youtube.com	ok	**IP:** 64.233.164.198 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.ig.smb.lead	ok	No Geolocation information available.
developer.android.com	ok	**IP:** 74.125.205.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
m.facebook.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
privacycenter.instagram.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
www.shops.fb	ok	No Geolocation information available.
www.bloks.commerce.shoppingcart	ok	No Geolocation information available.
www.bk.commerce.ratings	ok	No Geolocation information available.
secure.facebook.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
www.fbpay.hub	ok	No Geolocation information available.
goo.gle	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
i.s	ok	No Geolocation information available.
www.fxcal.settings.async	ok	No Geolocation information available.
t.me	ok	**IP:** 149.154.167.99 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Lowestoft **Latitude:** 52.475201 **Longitude:** 1.751590 **View:** Google Map
www.bloks.commerce.onboarding.adscredit.progress	ok	No Geolocation information available.
www.commerce.affiliate.discovery.home	ok	No Geolocation information available.
arxiv.org	ok	**IP:** 128.84.21.199 **Country:** United States of America **Region:** New York **City:** East Ithaca **Latitude:** 42.439522 **Longitude:** -76.478554 **View:** Google Map
msngr.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
fb.facebook.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
.facebook.com	ok	No Geolocation information available.
en.wikipedia.org	ok	**IP:** 91.198.174.192 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.instagram.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
fbplugins.herokuapp.com	ok	**IP:** 23.22.130.173 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.privacy.consent.prompt.action	ok	No Geolocation information available.
www.yp.supervision	ok	No Geolocation information available.
www.bloks.commerce.checkout	ok	No Geolocation information available.
www.bloks.commerce.media-grid	ok	No Geolocation information available.
i.instagram.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
www.orders	ok	No Geolocation information available.
www.facebook.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	ok	**IP:** 74.50.61.58 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.814899 **Longitude:** -96.879204 **View:** Google Map
portal.fb.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
mtouch.s	ok	No Geolocation information available.
graph.s	ok	No Geolocation information available.
mobile.facebook.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
www.ig.smb.services.lead	ok	No Geolocation information available.
fburl.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.bloks.commerce.shop.inventory.settings	ok	No Geolocation information available.
www.bloks.cxf.cpdp	ok	No Geolocation information available.
www.commerce.product.picker.product.source	ok	No Geolocation information available.
accounts.google.com	ok	**IP:** 173.194.220.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.minishops.pagelink	ok	No Geolocation information available.
www.fbpay.transaction	ok	No Geolocation information available.
www.ig.ixt.triggers.bottom	ok	No Geolocation information available.
fb.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
www.yp.familycenter.async	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 83.166.144.67 **Country:** Switzerland **Region:** Geneve **City:** Carouge **Latitude:** 46.180962 **Longitude:** 6.139210 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
www.bloks.cxf.cpdpcom.bloks.www.bloks.cxf.cpdp-instagram	ok	No Geolocation information available.
www.android.com	ok	**IP:** 74.125.205.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
docs.google.com	ok	**IP:** 64.233.163.194 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.example.com	ok	**IP:** 93.184.216.34 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
paypal.me	ok	**IP:** 64.4.250.36 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
lookaside.facebook.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
instagram.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
checkout.shopifycs.com	ok	**IP:** 34.120.248.174 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.bloks.commerce.order	ok	No Geolocation information available.
www.fx.settings.tyi.oauth	ok	No Geolocation information available.
fblitho.com	ok	**IP:** 172.67.222.89 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
www.fxcal.link.async	ok	No Geolocation information available.
www.bloks.commerce.shoppingcart.merchantview	ok	No Geolocation information available.
www.avatar.launcher	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.openstreetmap.org	ok	**IP:** 130.117.76.12 **Country:** United States of America **Region:** Georgia **City:** Atlanta **Latitude:** 33.749001 **Longitude:** -84.387978 **View:** Google Map
www.google.com	ok	**IP:** 64.233.162.105 **Country:** Brazil **Region:** Sao Paulo **City:** Sao Paulo **Latitude:** -23.547501 **Longitude:** -46.636108 **View:** Google Map
scontent-sjc3-1.cdninstagram.com	ok	**IP:** 78.29.1.40 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map

EMAILS

EMAIL	FILE
your.account@domain.com	com/OM7753/acra/ErrorReporter.java

TRACKERS

TRACKER	CATEGORIES	URL
Facebook Flipper	Analytics	https://reports.exodus-privacy.eu.org/trackers/392
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67

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.