ANDROID STATIC ANALYSIS REPORT

WhatsApp (2.22.17.76)

File Name:	Fouad.Whats9.45_By-FouadMODS.apk
Package Name:	com.whatsapp
Scan Date:	Nov. 30, 2022, 1:13 p.m.
App Security Score:	39/100 (HIGH RISK)
Grade:	C
Trackers Detection:	1/428

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
25	94	0	0	2

FILE INFORMATION

File Name: Fouad.Whats9.45_By-FouadMODS.apk
Size: 55.05MB
MD5: 1f19d2a028e5273950e4f47b2e0186d5
SHA1: 710ace45c76604dffb3b84d8488f1c6bde15aa07
SHA256: 32c167e3ec83cbf8bda514fb9a32d7fda21b65a96ed8f4a9720e82ff152b995b

APP INFORMATION

App Name: WhatsApp
Package Name: com.whatsapp
Main Activity: com.whatsapp.settings.SettingsNotifications
Target SDK: 29
Min SDK: 16
Max SDK:
Android Version Name: 2.22.17.76

Android Version Code: 999999999

APP COMPONENTS

Activities: 383
Services: 40
Receivers: 37
Providers: 7
Exported Activities: 99
Exported Services: 6
Exported Receivers: 14
Exported Providers: 3

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
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_PHONE_NUMBERS	dangerous		Allows read access to the device's phone number(s). This is a subset of the capabilities granted by READ_PHONE_STATE but is exposed to instant applications.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.
android.permission.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.INSTALL_SHORTCUT	normal		Allows an application to install a shortcut in Launcher.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.MANAGE_OWN_CALLS	normal		Allows a calling application which manages it own calls through the self-managed ConnectionService APIs.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
android.permission.READ_SYNC_SETTINGS	normal	read sync settings	Allows an application to read the sync settings, such as whether sync is enabled for Contacts.
android.permission.READ_SYNC_STATS	normal	read sync statistics	Allows an application to read the sync stats; e.g. the history of syncs that have occurred.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.SCHEDULE_EXACT_ALARM	normal		Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WRITE_SYNC_SETTINGS	normal	write sync settings	Allows an application to modify the sync settings, such as whether sync is enabled for Contacts.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
android.permission.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.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.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.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.whatsapp.permission.BROADCAST	unknown	Unknown permission	Unknown permission from android reference
com.whatsapp.permission.MAPS_RECEIVE	unknown	Unknown permission	Unknown permission from android reference
com.whatsapp.permission.REGISTRATION	unknown	Unknown permission	Unknown permission from android reference
com.whatsapp.sticker.READ	unknown	Unknown permission	Unknown permission from android reference
com.facebook.services.identity.FEO2	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.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>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check
Build.TAGS 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-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>
<tr><td>classes2.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
SIM operator check
network operator name check
emulator file 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>classes5.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table></td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.whatsapp.payments.receiver.IndiaUpiPayIntentReceiverActivity	Schemes: upi://, Hosts: pay,
com.whatsapp.TextAndDirectChatDeepLink	Schemes: http://, https://, whatsapp://, whatsapp-consumer://, Hosts: api.whatsapp.com, wa.me, send, catalog, product, message, pay, stickerpack, settings, qr, archive_settings, disappearing_messages, tos, support, directory, guia, ph, biztools,
com.whatsapp.Conversation	Schemes: sms://, smsto://,
com.whatsapp.registration.VerifyPhoneNumber	Schemes: whatsapp://, Hosts: r,
com.whatsapp.VerifySmsDeepLink	Schemes: http://, https://, Hosts: v.whatsapp.com,
com.whatsapp.HomeActivity	Schemes: whatsapp://, http://, https://, Hosts: chat, call, call.whatsapp.com, status, Mime Types: application/com.whatsapp.chat, application/com.whatsapp.join,
com.whatsapp.AcceptInviteLinkActivityDeepLink	Schemes: http://, https://, Hosts: chat.whatsapp.com,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.

CERTIFICATE ANALYSIS

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.

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Launch Mode of activity (com.whatsapp.businessdirectory.view.activity.BusinessDirectoryActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
4	Launch Mode of activity (com.whatsapp.payments.ui.BrazilViralityLinkVerifierActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
5	Launch Mode of activity (com.whatsapp.payments.ui.NoviSharedPaymentSettingsActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
6	Launch Mode of activity (com.whatsapp.payments.ui.ViralityLinkVerifierActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Activity (com.whatsapp.accountsync.CallContactLandingActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.CALL_PHONE [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. 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.
8	Broadcast Receiver (com.whatsapp.AlarmBroadcastReceiver) is Protected by a permission. Permission: com.whatsapp.permission.BROADCAST protectionLevel: signature [android:exported=true]	info	A Broadcast Receiver is found to be exported, but is protected by permission.
9	Launch Mode of activity (com.whatsapp.gallery.MediaGalleryActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

NO	ISSUE	SEVERITY	DESCRIPTION
10	TaskAffinity is set for activity (com.whatsapp.voipcalling.VoipActivityV2)	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.
11	Launch Mode of activity (com.whatsapp.voipcalling.VoipActivityV2) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
12	Launch Mode of activity (com.whatsapp.biz.catalog.view.activity.CatalogCategoryTabsActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
13	Launch Mode of activity (com.whatsapp.migration.export.ui.ExportMigrationActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

NO	ISSUE	SEVERITY	DESCRIPTION
14	Activity (com.whatsapp.migration.export.ui.ExportMigrationActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.apple.movetoios.ACCESS [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. 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.whatsapp.migration.export.api.ExportMigrationContentProvider) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.apple.movetoios.ACCESS [android:exported=true]	warning	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. 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
16	Launch Mode of activity (com.whatsapp.migration.export.ui.ExportMigrationDataExportedActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
17	Broadcast Receiver (com.whatsapp.migration.android.api.DeferredRestoreBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BACKUP [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.
18	Activity-Alias (com.whatsapp.0) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
19	Activity-Alias (com.whatsapp.1) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
20	Activity-Alias (com.whatsapp.2) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
21	Activity-Alias (com.whatsapp.3) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
22	Activity-Alias (com.whatsapp.4) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
23	Activity-Alias (com.whatsapp.5) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
24	Activity-Alias (com.whatsapp.6) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
25	Activity-Alias (com.whatsapp.7) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
26	Activity-Alias (com.whatsapp.8) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
27	Activity-Alias (com.whatsapp.9) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
28	Activity-Alias (com.whatsapp.10) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
29	Activity-Alias (com.whatsapp.11) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
30	Activity-Alias (com.whatsapp.12) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
31	Activity-Alias (com.whatsapp.13) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
32	Activity-Alias (com.whatsapp.14) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
33	Activity-Alias (com.whatsapp.15) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
34	Activity-Alias (com.whatsapp.16) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
35	Activity-Alias (com.whatsapp.17) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
36	Activity-Alias (com.whatsapp.18) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
37	Activity-Alias (com.whatsapp.19) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
38	Activity-Alias (com.whatsapp.20) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
39	Activity-Alias (com.whatsapp.21) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
40	Activity-Alias (com.whatsapp.22) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
41	Activity-Alias (com.whatsapp.23) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
42	Activity-Alias (com.whatsapp.24) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
43	Activity-Alias (com.whatsapp.25) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
44	Activity-Alias (com.whatsapp.26) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
45	Activity-Alias (com.whatsapp.27) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
46	Activity-Alias (com.whatsapp.28) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
47	Activity-Alias (com.whatsapp.29) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
48	Activity-Alias (com.whatsapp.30) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
49	Activity-Alias (com.whatsapp.31) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
50	Activity-Alias (com.whatsapp.32) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
51	Activity-Alias (com.whatsapp.33) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
52	Activity-Alias (com.whatsapp.34) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
53	Activity-Alias (com.whatsapp.35) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
54	Activity-Alias (com.whatsapp.36) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
55	Activity-Alias (com.whatsapp.37) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
56	Activity-Alias (com.whatsapp.38) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
57	Activity-Alias (com.whatsapp.39) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
58	Activity-Alias (com.whatsapp.40) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
59	Activity-Alias (com.whatsapp.41) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
60	Activity-Alias (com.whatsapp.42) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
61	Activity-Alias (com.whatsapp.43) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
62	Activity-Alias (com.whatsapp.44) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
63	Activity-Alias (com.whatsapp.45) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
64	Activity-Alias (com.whatsapp.46) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
65	Activity-Alias (com.whatsapp.47) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
66	Activity-Alias (com.whatsapp.48) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
67	Activity-Alias (com.whatsapp.49) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
68	Activity-Alias (com.whatsapp.50) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
69	Activity-Alias (com.whatsapp.51) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
70	Activity-Alias (com.whatsapp.52) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
71	Activity-Alias (com.whatsapp.53) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
72	Activity-Alias (com.whatsapp.54) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
73	Activity-Alias (com.whatsapp.55) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
74	Activity-Alias (com.whatsapp.56) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
75	Activity-Alias (com.whatsapp.57) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
76	Activity-Alias (com.whatsapp.58) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
77	Activity-Alias (com.whatsapp.59) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
78	Activity-Alias (com.whatsapp.60) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
79	Activity-Alias (com.whatsapp.61) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
80	Activity-Alias (com.whatsapp.62) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
81	Activity-Alias (com.whatsapp.63) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
82	Activity-Alias (com.whatsapp.64) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
83	Activity-Alias (com.whatsapp.65) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
84	Activity-Alias (com.whatsapp.66) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
85	Activity-Alias (com.whatsapp.67) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
86	Activity-Alias (com.whatsapp.68) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
87	Activity-Alias (com.whatsapp.69) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
88	Activity-Alias (com.whatsapp.70) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
89	Activity-Alias (com.whatsapp.71) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
90	Activity-Alias (com.whatsapp.72) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
91	Activity-Alias (com.whatsapp.73) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
92	Activity-Alias (com.whatsapp.74) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
93	Activity-Alias (com.whatsapp.75) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.
94	Launch Mode of activity (com.whatsapp.registration.EULA) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

NO	ISSUE	SEVERITY	DESCRIPTION
95	Launch Mode of activity (com.whatsapp.registration.RegisterPhone) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
96	Launch Mode of activity (com.whatsapp.registration.VerifyPhoneNumber) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
97	Launch Mode of activity (com.whatsapp.registration.PrimaryFlashCallEducationScreen) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
98	Launch Mode of activity (com.whatsapp.registration.VerifyTwoFactorAuth) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

NO	ISSUE	SEVERITY	DESCRIPTION
99	Launch Mode of activity (com.whatsapp.registration.RegisterName) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
100	Launch Mode of activity (com.whatsapp.HomeActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
101	Launch Mode of activity (com.whatsapp.notification.PopupNotification) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
102	Launch Mode of activity (com.whatsapp.messaging.CaptivePortalActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

NO	ISSUE	SEVERITY	DESCRIPTION
103	Launch Mode of activity (com.whatsapp.camera.CameraActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
104	TaskAffinity is set for activity (com.whatsapp.camera.LauncherCameraActivity)	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.
105	Launch Mode of activity (com.whatsapp.corruptinstallation.CorruptInstallationActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
106	TaskAffinity is set for activity (com.whatsapp.VoiceMessagingActivity)	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
107	Launch Mode of activity (com.whatsapp.authentication.AppAuthenticationActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
108	TaskAffinity is set for activity (com.whatsapp.biz.product.view.activity.ProductDetailActivity)	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.
109	Launch Mode of activity (com.whatsapp.userban.ui.BanAppealActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
110	Broadcast Receiver (com.whatsapp.registration.RegistrationCompletedReceiver) is Protected by a permission. Permission: com.whatsapp.permission.REGISTRATION protectionLevel: signature [android:exported=true]	info	A Broadcast Receiver is found to be exported, but is protected by permission.

NO	ISSUE	SEVERITY	DESCRIPTION
111	Broadcast Receiver (com.whatsapp.registration.directmigration.MigrationProviderOrderedBroadcastReceiver) is Protected by a permission. Permission: com.whatsapp.permission.REGISTRATION protectionLevel: signature [android:exported=true]	info	A Broadcast Receiver is found to be exported, but is protected by permission.
112	Broadcast Receiver (com.whatsapp.registration.directmigration.MigrationRequesterBroadcastReceiver) is Protected by a permission. Permission: com.whatsapp.permission.REGISTRATION protectionLevel: signature [android:exported=true]	info	A Broadcast Receiver is found to be exported, but is protected by permission.
113	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
114	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.
115	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.

NO	ISSUE	SEVERITY	DESCRIPTION
116	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.
117	Service (androidx.sharetarget.ChooserTargetServiceCompat) 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.
118	Broadcast Receiver (com.whatsapp.yo.WidgetProvider) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
119	Broadcast Receiver (com.whatsapp.yo.autoschedreply.Receiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

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/libunwindstack.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.
2	lib/armeabi-v7a/libsoundtouch.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/libopustool.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.
4	lib/armeabi-v7a/libsuperpack.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/arm64-v8a/libunwindstack.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.
6	lib/arm64-v8a/libsoundtouch.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
7	lib/arm64-v8a/libopustool.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__strcpy_chk', '__strlen_chk', '__vsnprintf_chk']	True info Symbols are stripped.
8	lib/arm64-v8a/libsuperpack.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__vsnprintf_chk', '__memcpy_chk', '__strcpy_chk']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
novi.com	ok	**IP:** 31.13.72.8 **Country:** Sweden **Region:** Stockholms lan **City:** Stockholm **Latitude:** 59.332581 **Longitude:** 18.064899 **View:** Google Map
www.yousefalbasha.com	ok	**IP:** 172.64.105.32 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
yousefalbasha.com	ok	**IP:** 172.64.105.32 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
whatsapp.com	ok	**IP:** 31.13.72.52 **Country:** Sweden **Region:** Stockholms lan **City:** Stockholm **Latitude:** 59.332581 **Longitude:** 18.064899 **View:** Google Map
www.exemplo.com	ok	**IP:** 99.83.248.67 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
www.novi.com	ok	**IP:** 157.240.205.1 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.whatsapp.com	ok	**IP:** 157.240.205.60 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
theyocraft.com	ok	No Geolocation information available.

TRACKERS

TRACKER	CATEGORIES	URL
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48

HARDCODED SECRETS

POSSIBLE SECRETS
"account_sync_authenticating" : "Authenticating"
"app_auth_disabled" : "Disabled"
"app_auth_timeout_immediately" : "Immediately"
"encrypted_backup_encryption_key_info_button_continue" : "Continue"
"encrypted_backup_restore_encryption_key_input_next_button" : "Next"
"google_api_key" : "AIzaSyCGOJbGQ95SWrXxl8wk-_cRQZcJl42bvDU"
"google_crash_reporting_api_key" : "AIzaSyCGOJbGQ95SWrXxl8wk-_cRQZcJl42bvDU"
"instrumentation_auth_perm_button" : "Next"
"maps_key" : "0YfjKhnxK4BnAuGV-Sq20174g6HG1YYFLerDEDA"

POSSIBLE SECRETS
"settings_gdrive_authenticating_with_google_servers_title" : "Authenticating…"
"settings_two_factor_auth_disable" : "Disable"
"settings_two_factor_auth_enable" : "Enable"
"two_factor_auth_disabling" : "Disabling…"
"two_factor_auth_submit" : "Save"
"donations__bitcoin" : "Bitcoin"
"settings_two_factor_auth" : "Totrinsgodkendelse"
"instrumentation_auth_title" : "WhatsApp□□□□"
"settings_two_factor_auth" : "2□□□□"
"settings_two_factor_auth" : "Tweestapverifikasie"
"settings_two_factor_auth" : "■■■■■■■■■■■■■■■■■■■■■■"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"
"donations__bitcoin" : "Bitcoin"

POSSIBLE SECRETS
"settings_two_factor_auth" : "Tvåstegsverifiering"
"donations__bitcoin" : "ביטקוין"
"donations__bitcoin" : "Bitcoin"
"settings_two_factor_auth" : "□□□□"
"settings_two_factor_auth" : "□□□□"
"donations__bitcoin" : "Bitcoin"
"settings_two_factor_auth" : "□□□□□"

PLAYSTORE INFORMATION

Title: WhatsApp Messenger

Score: 4.265918 **Installs:** 5,000,000,000+ **Price:** 0 **Android Version Support:** **Category:** Communication **Play Store URL:** com.whatsapp

Developer Details: WhatsApp LLC, WhatsApp+LLC, 1601 Willow Road Menlo Park, CA 94025, http://www.whatsapp.com/, android@support.whatsapp.com,

Release Date: Oct 18, 2010 **Privacy Policy:** Privacy link

Description:

WhatsApp from Meta is a FREE messaging and video calling app. It’s used by over 2B people in more than 180 countries. It’s simple, reliable, and private, so you can easily keep in touch with your friends and family. WhatsApp works across mobile and desktop even on slow connections, with no subscription fees*. Private messaging across the world Your personal messages and calls to friends and family are end-to-end encrypted. No one outside of your chats, not even WhatsApp, can read or listen to them. Simple and secure connections, right away All you need is your phone number, no user names or logins. You can quickly view your contacts who are on WhatsApp and start messaging. High quality voice and video calls Make secure video and voice calls with up to 8 people for free*. Your calls work across mobile devices using your phone’s Internet service, even on slow connections. Group chats to keep you in contact Stay in touch with your friends and family. End-to-end encrypted group chats let you share messages, photos, videos and documents across mobile and desktop. Stay connected in real time Share your location with only those in your individual or group chat, and stop sharing at any time. Or record a voice message to connect quickly. Share daily moments through Status Status allows you to share text, photos, video and GIF updates that disappear after 24 hours. You can choose to share status posts with all your contacts or just selected ones. *Data charges may apply. Contact your provider for details. -- If you have any feedback or questions, please go to WhatsApp > Settings > Help > Contact Us

Report Generated by - MobSF v3.6.2 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.