MOBSF

ANDROID STATIC ANALYSIS REPORT

Telegram Beta (12.2.0)

File Name:	telegram_.apk

Package Name:	org.telegram.messenger.beta
Scan Date:	Nov. 8, 2025, 8:20 p.m.
App Security Score:	48/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	52	5	2	1

FILE INFORMATION

File Name: telegram_.apk
Size: 78.53MB
MD5: ab530014ea29f199753432b8635cbf14
SHA1: 2866cf31b9c5755d3841660fd187030f6f9f3c17
SHA256: bcbf75b91bdfc71efa5f6b069da98161b37103f52e416829b019a707a51073c5

APP INFORMATION

App Name: Telegram Beta
Package Name: org.telegram.messenger.beta
Main Activity: org.telegram.ui.LaunchActivity
Target SDK: 35
Min SDK: 21
Max SDK:
Android Version Name: 12.2.0
Android Version Code: 62369

APP COMPONENTS

Activities: 18
Services: 29

Receivers: 27
Providers: 6
Exported Activities: 15
Exported Services: 15
Exported Receivers: 5
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: L=Saint-Petersburg, O=VK, OU=VK, CN=Nikolay Kudashov
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-08-29 19:13:13+00:00
Valid To: 2038-08-23 19:13:13+00:00
Issuer: L=Saint-Petersburg, O=VK, OU=VK, CN=Nikolay Kudashov
Serial Number: 0x521f9d49
Hash Algorithm: sha1
md5: 26babc62540ef0c20bfc6bacf3d3b1f5
sha1: 9723e5838612e9c7c08ca2c6573b6026d7a51f8f
sha256: 49c1522548ebacd46ce322b6fd47f6092bb745d0f88082145caf35e14dcc38e1
sha512: b47593b965b36396b06296546de386e452f84180968bca894ac90c5dfdbdedae97c3701f0454ec90f1a616e0bb5ab2c8b4bd8efdbd7b8649268fc7b1f614d648
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 5a75db88b7dde612c71b129469a376894dee2c4d8c3266380b658d837ee46677
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

PERMISSION	STATUS	INFO	DESCRIPTION
org.telegram.messenger.beta.permission.MAPS_RECEIVE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_MEDIA_LOCATION	dangerous	access any geographic locations	Allows an application to access any geographic locations persisted in the user's shared collection.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.READ_CLIPBOARD	unknown	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	normal	enables foreground services for media playback.	Allows a regular application to use Service.startForeground with the type "mediaPlayback".
android.permission.FOREGROUND_SERVICE_MEDIA_PROJECTION	normal	allows foreground services for media projection.	Allows a regular application to use Service.startForeground with the type "mediaProjection".
android.permission.FOREGROUND_SERVICE_CAMERA	normal	allows foreground services with camera use.	Allows a regular application to use Service.startForeground with the type "camera".
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
android.permission.FOREGROUND_SERVICE_MICROPHONE	normal	permits foreground services with microphone use.	Allows a regular application to use Service.startForeground with the type "microphone".
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
android.permission.READ_MEDIA_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
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.
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.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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.INSTALL_SHORTCUT	normal	permits installation of shortcuts in Launcher.	Allows an application to install a shortcut in Launcher.
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
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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.MANAGE_OWN_CALLS	normal	enables a calling app to manage its own calls.	Allows a calling application which manages it own calls through the self-managed ConnectionService APIs.
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.READ_PHONE_NUMBERS	dangerous	allows reading of the device's phone number(s).	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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.
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.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
org.telegram.messenger.beta.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator check
network operator name check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes3.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check device ID check subscriber ID check ro.hardware check ro.product.device check ro.kernel.qemu check emulator file check possible VM check</td></tr><tr><td>Compiler</td><td>r8</td></tr></table>
classes4.dex	<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>r8</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check
Build.HARDWARE check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>lib/arm64-v8a/libtmessages.49.so</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>anti_hook</td><td>syscalls</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.microsoft.appcenter.distribute.DeepLinkActivity	Schemes: appcenter://, Hosts: updates, Paths: /,
org.telegram.ui.LaunchActivity	Schemes: http://, https://, tonsite://, tg://, Hosts: telegram.me, telegram.dog, t.me, Mime Types: image/*, video/*, text/plain, */*, vnd.android.cursor.item/vnd.org.telegram.messenger.android.profile,
org.telegram.ui.ShareActivity	Schemes: tgb://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 2 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

HIGH: 2 | WARNING: 39 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	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.
4	Service (org.telegram.messenger.GcmPushListenerService) is not Protected. [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.
5	Service (org.telegram.messenger.GoogleVoiceClientService) is not Protected. [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.
6	Activity (org.telegram.messenger.GoogleVoiceClientActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Activity (com.microsoft.appcenter.distribute.DeepLinkActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Broadcast Receiver (com.microsoft.appcenter.distribute.DownloadManagerReceiver) is not Protected. [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.
9	Activity-Alias (org.telegram.messenger.DefaultIcon) is not Protected. [android:exported=true]	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.
10	Activity-Alias (org.telegram.messenger.VintageIcon) is not Protected. [android:exported=true]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
11	Activity-Alias (org.telegram.messenger.AquaIcon) is not Protected. [android:exported=true]	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.
12	Activity-Alias (org.telegram.messenger.PremiumIcon) is not Protected. [android:exported=true]	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.
13	Activity-Alias (org.telegram.messenger.TurboIcon) is not Protected. [android:exported=true]	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.
14	Activity-Alias (org.telegram.messenger.NoxIcon) is not Protected. [android:exported=true]	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.
15	Activity-Alias (org.telegram.ui.CallsActivity) 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-Alias 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.
16	Activity (org.telegram.ui.ShareActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
17	Activity (org.telegram.ui.ExternalActionActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
18	Activity (org.telegram.ui.ChatsWidgetConfigActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
19	Activity (org.telegram.ui.ContactsWidgetConfigActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
20	Activity (org.telegram.messenger.OpenChatReceiver) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
21	Activity (org.telegram.messenger.OpenAttachedMenuBotReceiver) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
22	TaskAffinity is set for activity (org.telegram.ui.VoIPPermissionActivity)	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.
23	TaskAffinity is set for activity (org.telegram.ui.VoIPFeedbackActivity)	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.
24	Broadcast Receiver (org.telegram.messenger.SmsReceiver) is not Protected. [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.
25	Service (org.telegram.messenger.AuthenticatorService) is not Protected. [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.
26	Service (org.telegram.messenger.ContactsSyncAdapterService) is not Protected. [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.
27	Service (org.telegram.messenger.BringAppForegroundService) is not Protected. [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.
28	Service (org.telegram.messenger.NotificationsService) is not Protected. [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.
29	Service (org.telegram.messenger.VideoEncodingService) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
30	Service (org.telegram.ui.Stories.recorder.StoryUploadingService) is not Protected. [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.
31	Service (org.telegram.messenger.ImportingService) is not Protected. [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.
32	Service (org.telegram.messenger.LocationSharingService) is not Protected. [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.
33	Service (org.telegram.messenger.MusicPlayerService) is not Protected. [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.
34	Service (org.telegram.messenger.MusicBrowserService) is not Protected. [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.
35	Service (org.telegram.messenger.voip.TelegramConnectionService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_TELECOM_CONNECTION_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.
36	Broadcast Receiver (org.telegram.messenger.RefererReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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.
37	Content Provider (org.telegram.messenger.voip.CallNotificationSoundProvider) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
38	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.
39	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.
40	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.
41	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 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.

</> CODE ANALYSIS

HIGH: 2 | WARNING: 9 | INFO: 4 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/microsoft/appcenter/AbstractAppCenterService.java com/microsoft/appcenter/AppCenter.java com/microsoft/appcenter/Constants.java com/microsoft/appcenter/CustomProperties.java com/microsoft/appcenter/Flags.java com/microsoft/appcenter/ServiceInstrumentationUtils.java com/microsoft/appcenter/UncaughtExceptionHandler.java com/microsoft/appcenter/analytics/Analytics.java com/microsoft/appcenter/analytics/channel/AnalyticsValidator.java com/microsoft/appcenter/analytics/channel/SessionTracker.java com/microsoft/appcenter/analytics/ingestion/models/EventLog.java com/microsoft/appcenter/analytics/ingestion/models/json/EventLogFactory.java com/microsoft/appcenter/channel/DefaultChannel.java com/microsoft/appcenter/channel/OneCollectorChannelListener.java com/microsoft/appcenter/crashes/Crashes.java com/microsoft/appcenter/crashes/WrapperSdkExceptionManager.java com/microsoft/appcenter/crashes/ingestion/models/AbstractErrorLog.java com/microsoft/appcenter/crashes/ingestion/models/ErrorAttachmentLog.java com/microsoft/appcenter/crashes/ingestion/models/HandledErrorLog.java com/microsoft/appcenter/crashes/ingestion/models/ManagedErrorLog.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/microsoft/appcenter/distribute/BrowserUtils.java com/microsoft/appcenter/distribute/DeepLinkActivity.java com/microsoft/appcenter/distribute/Distribute.java com/microsoft/appcenter/distribute/DistributeUtils.java com/microsoft/appcenter/distribute/InstallerUtils.java com/microsoft/appcenter/distribute/ReleaseDownloadListener.java com/microsoft/appcenter/distribute/ResumeFromBackgroundTask.java com/microsoft/appcenter/distribute/download/manager/DownloadManagerReleaseDownloader.java com/microsoft/appcenter/distribute/download/manager/DownloadManagerRequestTask.java com/microsoft/appcenter/http/AbstractAppCallTemplate.java com/microsoft/appcenter/http/DefaultHttpClient.java com/microsoft/appcenter/http/DefaultHttpClientCallTask.java com/microsoft/appcenter/http/HttpClientNetworkStateHandler.java com/microsoft/appcenter/http/HttpClientRetryer.java com/microsoft/appcenter/ingestion/OneCollectorIngestion.java com/microsoft/appcenter/ingestion/models/AbstractLog.java com/microsoft/appcenter/ingestion/models/one/CommonSchemaDataUtils.java com/microsoft/appcenter/ingestion/models/one/CommonSchemaLog.java com/microsoft/appcenter/ingestion/models/one/PartAUtils.java com/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/utils/AppCenterLog.java com/microsoft/appcenter/utils/AsyncTaskUtils.java com/microsoft/appcenter/utils/DeviceInfoHelper.java com/microsoft/appcenter/utils/IdHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/microsoft/appcenter/utils/NetworkStateHelper.java com/microsoft/appcenter/utils/context/SessionContext.java com/microsoft/appcenter/utils/context/UserIdContext.java com/microsoft/appcenter/utils/crypto/CryptoUtils.java com/microsoft/appcenter/utils/storage/DatabaseManager.java com/microsoft/appcenter/utils/storage/FileManager.java me/vkryl/android/animator/FactorAnimator.java org/telegram/DispatchQueuePriority.java org/telegram/PhoneFormat/PhoneFormat.java org/telegram/SQLite/SQLiteCursor.java org/telegram/SQLite/SQLiteDatabase.java org/telegram/SQLite/SQLitePreparedStatement.java org/telegram/messenger/AndroidUtilities.java org/telegram/messenger/AnimatedFileDrawableStream.java org/telegram/messenger/AppGlobalConfig.java org/telegram/messenger/ApplicationLoader.java org/telegram/messenger/ApplicationLoaderImpl.java org/telegram/messenger/AuthTokensHelper.java org/telegram/messenger/AutoDeleteMediaTask.java org/telegram/messenger/BetaUpdaterController.java org/telegram/messenger/BillingController.java org/telegram/messenger/BirthdayController.java org/telegram/messenger/BotForumHelper.java org/telegram/messenger/BuildVars.java org/telegram/messenger/CaptchaController.java org/telegram/messenger/ChatObject.java org/telegram/messenger/ChatThemeController.java org/telegram/messenger/ChatsRemoteViewsFactory.java org/telegram/messenger/CodeHighlighting.java org/telegram/messenger/ContactsController.java org/telegram/messenger/ContactsRemoteViewsFactory.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/telegram/messenger/ContactsSyncAdapterService.java org/telegram/messenger/DatabaseMigrationHelper.java org/telegram/messenger/DispatchQueue.java org/telegram/messenger/DispatchQueuePoolBackground.java org/telegram/messenger/DocumentObject.java org/telegram/messenger/DownloadController.java org/telegram/messenger/Emoji.java org/telegram/messenger/EmuInputDevicesDetector.java org/telegram/messenger/FactCheckController.java org/telegram/messenger/FeedRemoteViewsFactory.java org/telegram/messenger/FileLoadOperation.java org/telegram/messenger/FileLoader.java org/telegram/messenger/FileLog.java org/telegram/messenger/FilePathDatabase.java org/telegram/messenger/FileRefController.java org/telegram/messenger/FileStreamLoadOperation.java org/telegram/messenger/FileUploadOperation.java org/telegram/messenger/FilesMigrationService.java org/telegram/messenger/FingerprintController.java org/telegram/messenger/GcmPushListenerService.java org/telegram/messenger/ImageLoader.java org/telegram/messenger/ImageReceiver.java org/telegram/messenger/ImportingService.java org/telegram/messenger/KeepAliveJob.java org/telegram/messenger/LanguageDetector.java org/telegram/messenger/LinkifyPort.java org/telegram/messenger/LiteMode.java org/telegram/messenger/LocaleController.java org/telegram/messenger/LocationController.java org/telegram/messenger/LocationSharingService.java org/telegram/messenger/MediaController.java org/telegram/messenger/MediaDataController.java org/telegram/messenger/MessageObject.java org/telegram/messenger/MessagePreviewParams.java org/telegram/messenger/MessagesController.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/telegram/messenger/MessagesStorage.java org/telegram/messenger/MusicBrowserService.java org/telegram/messenger/MusicPlayerService.java org/telegram/messenger/NativeLoader.java org/telegram/messenger/NotchInfoUtils.java org/telegram/messenger/NotificationBadge.java org/telegram/messenger/NotificationCenter.java org/telegram/messenger/NotificationDismissReceiver.java org/telegram/messenger/NotificationImageProvider.java org/telegram/messenger/NotificationsController.java org/telegram/messenger/NotificationsDisabledReceiver.java org/telegram/messenger/OpenAttachedMenuBotReceiver.java org/telegram/messenger/OpenChatReceiver.java org/telegram/messenger/PushListenerController.java org/telegram/messenger/SavedMessagesController.java org/telegram/messenger/ScreenReceiver.java org/telegram/messenger/SecretChatHelper.java org/telegram/messenger/SendMessagesHelper.java org/telegram/messenger/SharedConfig.java org/telegram/messenger/SmsReceiver.java org/telegram/messenger/SvgHelper.java org/telegram/messenger/Timer.java org/telegram/messenger/TopicsController.java org/telegram/messenger/TranslateController.java org/telegram/messenger/UnconfirmedAuthController.java org/telegram/messenger/UserConfig.java org/telegram/messenger/UserNameResolver.java org/telegram/messenger/Utilities.java org/telegram/messenger/VideoEditedInfo.java org/telegram/messenger/VideoEncodingService.java org/telegram/messenger/XiaomiUtilities.java org/telegram/messenger/audioinfo/OtherAudioInfo.java org/telegram/messenger/browser/Browser.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/telegram/messenger/browser/Browser.java org/telegram/messenger/camera/Camera2Session.java org/telegram/messenger/camera/CameraController.java org/telegram/messenger/camera/CameraSession.java org/telegram/messenger/camera/CameraView.java org/telegram/messenger/chromecast/ChromecastController.java org/telegram/messenger/chromecast/ChromecastFileServer.java org/telegram/messenger/pip/PipActivityController.java org/telegram/messenger/pip/PipActivityHandler.java org/telegram/messenger/pip/source/PipSourceHandlerState2.java org/telegram/messenger/ringtone/RingtoneDataStore.java org/telegram/messenger/secretmedia/ExtendedDefaultDataSource.java org/telegram/messenger/support/JobIntentService.java org/telegram/messenger/support/customtabsclient/shared/CustomTabsHelper.java org/telegram/messenger/support/fingerprint/FingerprintManagerCompatApi23.java org/telegram/messenger/utils/BillingUtilities.java org/telegram/messenger/utils/BitmapsCache.java org/telegram/messenger/utils/CopyUtilities.java org/telegram/messenger/video/AudioDecoder.java org/telegram/messenger/video/AudioRecoder.java org/telegram/messenger/video/MediaCodecVideoConvertor.java org/telegram/messenger/video/OutputSurface.java org/telegram/messenger/video/TextureRenderer.java org/telegram/messenger/video/VideoFramesRewinder.java org/telegram/messenger/video/VideoPlayerHolderBase.java org/telegram/messenger/video/WebmEncoder.java org/telegram/messenger/voip/AudioRecordJNI.java org/telegram/messenger/voip/AudioTrackJNI.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/telegram/messenger/voip/ConferenceCall.java org/telegram/messenger/voip/GroupCallMessagesController.java org/telegram/messenger/voip/Instance.java org/telegram/messenger/voip/JNIUtilities.java org/telegram/messenger/voip/NativeInstance.java org/telegram/messenger/voip/TelegramConnectionService.java org/telegram/messenger/voip/VideoCapturerDevice.java org/telegram/messenger/voip/VoIPDebugToSend.java org/telegram/messenger/voip/VoIPGroupNotification.java org/telegram/messenger/voip/VoIPPreNotificationService.java org/telegram/messenger/voip/VoIPServerConfig.java org/telegram/messenger/voip/VoIPService.java org/telegram/messenger/wallpaper/WallpaperGiftPatternPosition.java org/telegram/tgnet/ConnectionsManager.java org/telegram/tgnet/NativeByteBuffer.java org/telegram/tgnet/SerializedData.java org/telegram/tgnet/TLClassStore.java org/telegram/tgnet/TLParseException.java org/telegram/tgnet/TLRPC.java org/telegram/tgnet/json/TLJsonBuilder.java org/telegram/tgnet/json/TLJsonParser.java org/telegram/ui/AccountFrozenAlert.java org/telegram/ui/ActionBar/ActionBarLayout.java org/telegram/ui/ActionBar/ActionBarPopupWindow.java org/telegram/ui/ActionBar/AlertDialog.java org/telegram/ui/ActionBar/BaseFragment.java org/telegram/ui/ActionBar/BottomSheet.java org/telegram/ui/ActionBar/BottomSheetTabDialog.java org/telegram/ui/ActionBar/BottomSheetTabs.java org/telegram/ui/ActionBar/DrawerLayoutContainer.java org/telegram/ui/ActionBar/EmojiThemes.java org/telegram/ui/ActionBar/Theme.java org/telegram/ui/ActionBar/ThemeDescription.java org/telegram/ui/ActionIntroActivity.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	org/telegram/ui/Adapters/ContactsAdapter.java org/telegram/ui/Adapters/DialogsAdapter.java org/telegram/ui/Adapters/DialogsSearchAdapter.java org/telegram/ui/Adapters/SearchAdapter.java org/telegram/ui/Adapters/SearchAdapterHelper.java org/telegram/ui/ArticleViewer.java org/telegram/ui/BasePermissionsActivity.java org/telegram/ui/BubbleActivity.java org/telegram/ui/Business/BusinessLinksController.java org/telegram/ui/Business/BusinessRecipientsHelper.java org/telegram/ui/Business/LocationActivity.java org/telegram/ui/Business/QuickRepliesController.java org/telegram/ui/CacheControlActivity.java org/telegram/ui/CachedMediaLayout.java org/telegram/ui/CameraScanActivity.java org/telegram/ui/CastSync.java org/telegram/ui/Cells/AboutLinkCell.java org/telegram/ui/Cells/AudioPlayerCell.java org/telegram/ui/Cells/BaseCell.java org/telegram/ui/Cells/BotHelpCell.java org/telegram/ui/Cells/ChannelRecommendationsCell.java org/telegram/ui/Cells/ChatActionCell.java org/telegram/ui/Cells/ChatMessageCell.java org/telegram/ui/Cells/ContextLinkCell.java org/telegram/ui/Cells/DialogCell.java org/telegram/ui/Cells/DialogMeUrlCell.java org/telegram/ui/Cells/DrawerActionCell.java org/telegram/ui/Cells/DrawerProfileCell.java org/telegram/ui/Cells/ProfileChannelCell.java org/telegram/ui/Cells/SettingsSuggestionCell.java org/telegram/ui/Cells/SharedAudioCell.java org/telegram/ui/Cells/SharedLinkCell.java org/telegram/ui/Cells/TextSelectionHelper.java org/telegram/ui/Cells/ThemesHorizontalListCell.java org/telegram/ui/ChangeBioActivity.java org/telegram/ui/ChangeUsernameActivity.java org/telegram/ui/ChannelAdminLogActivity.java org/telegram/ui/ChannelColorActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/telegram/ui/ChannelCreateActivity.java org/telegram/ui/ChannelMonetizationLayout.java org/telegram/ui/ChatActivity.java org/telegram/ui/ChatEditActivity.java org/telegram/ui/ChatRightsEditActivity.java org/telegram/ui/ChatUsersActivity.java org/telegram/ui/Components/AlertsCreator.java org/telegram/ui/Components/AnimatedEmojiDrawable.java org/telegram/ui/Components/AnimatedFileDrawable.java org/telegram/ui/Components/AudioPlayerAlert.java org/telegram/ui/Components/AvatarDrawable.java org/telegram/ui/Components/BlurBehindDrawable.java org/telegram/ui/Components/ChatActivityEnterView.java org/telegram/ui/Components/ChatAttachAlert.java org/telegram/ui/Components/ChatAttachAlertAudioLayout.java org/telegram/ui/Components/ChatAttachAlertDocumentLayout.java org/telegram/ui/Components/ChatAttachAlertLocationLayout.java org/telegram/ui/Components/ChatAttachAlertPhotoLayout.java org/telegram/ui/Components/ChatAttachAlertPollLayout.java org/telegram/ui/Components/ChatAvatarContainer.java org/telegram/ui/Components/ChatThemeBottomSheet.java org/telegram/ui/Components/ClippingImageView.java org/telegram/ui/Components/Crop/CropView.java org/telegram/ui/Components/DialogsBotsAdapter.java org/telegram/ui/Components/DrawingInBackgroundThreadDrawable.java org/telegram/ui/Components/EarListener.java org/telegram/ui/Components/EditTextBoldCursor.java org/telegram/ui/Components/EditTextCaption.java org/telegram/ui/Components/EditTextEffects.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/telegram/ui/Components/EditTextEffects.java org/telegram/ui/Components/EditTextEmoji.java org/telegram/ui/Components/EmbedBottomSheet.java org/telegram/ui/Components/EmojiColorPickerWindow.java org/telegram/ui/Components/EmojiPacksAlert.java org/telegram/ui/Components/EmojiView.java org/telegram/ui/Components/FilterGLThread.java org/telegram/ui/Components/FilterShaders.java org/telegram/ui/Components/FireworksOverlay.java org/telegram/ui/Components/ForegroundDetector.java org/telegram/ui/Components/GroupCallPipAlertView.java org/telegram/ui/Components/GroupVoipInviteAlert.java org/telegram/ui/Components/ImageUpdater.java org/telegram/ui/Components/InstantCameraVideoEncoderOverlayHelper.java org/telegram/ui/Components/InstantCameraView.java org/telegram/ui/Components/JoinCallAlert.java org/telegram/ui/Components/LetterDrawable.java org/telegram/ui/Components/LinkActionView.java org/telegram/ui/Components/MentionsContainerView.java org/telegram/ui/Components/MessagePreviewView.java org/telegram/ui/Components/MotionBackgroundDrawable.java org/telegram/ui/Components/Paint/PaintTypeface.java org/telegram/ui/Components/Paint/RenderView.java org/telegram/ui/Components/Paint/Shader.java org/telegram/ui/Components/Paint/ShapeDetector.java org/telegram/ui/Components/Paint/Slice.java org/telegram/ui/Components/Paint/Texture.java org/telegram/ui/Components/Paint/Utils.java org/telegram/ui/Components/Paint/Views/LPhotoPaintView.java org/telegram/ui/Components/Paint/Views/PhotoVi

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ew.java org/telegram/ui/Components/Paint/Views/StickerMakerView.java org/telegram/ui/Components/PasscodeView.java org/telegram/ui/Components/PathAnimator.java org/telegram/ui/Components/PermissionRequest.java org/telegram/ui/Components/PhonebookShareAlert.java org/telegram/ui/Components/PhotoViewerWebView.java org/telegram/ui/Components/PipRoundVideoView.java org/telegram/ui/Components/Premium/GLIcon/GLIconTextureView.java org/telegram/ui/Components/Premium/PremiumAppIconsPreviewView.java org/telegram/ui/Components/Premium/PremiumFeatureBottomSheet.java org/telegram/ui/Components/Premium/PremiumNotAvailableBottomSheet.java org/telegram/ui/Components/Premium/boosts/ReassignBoostBottomSheet.java org/telegram/ui/Components/Premium/boosts/cells/msg/GiveawayResultsMessageCell.java org/telegram/ui/Components/ProfileGalleryView.java org/telegram/ui/Components/ProximitySheet.java org/telegram/ui/Components/QRCodeBottomSheet.java org/telegram/ui/Components/RLottieDrawable.java org/telegram/ui/Components/Reactions/ChatCustomReactionsEditActivity.java org/telegram/ui/Components/RecyclerListView.java org/telegram/ui/Components/SearchDownloadsContainer.java org/telegram/ui/Components/SeekBar.java org/telegram/ui/Components/SeekBarView.java org/telegram/ui/Components/ShareAlert.java org/telegram/ui/Components/SharedMediaLayout.java org/telegram/ui/Components/SizeNotifierFrameLayout.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/telegram/ui/Components/SlotsDrawable.java org/telegram/ui/Components/StaticLayoutEx.java org/telegram/ui/Components/StickerCategoriesListView.java org/telegram/ui/Components/StickersAlert.java org/telegram/ui/Components/TermsOfServiceView.java org/telegram/ui/Components/ThanosEffect.java org/telegram/ui/Components/ThemeEditorView.java org/telegram/ui/Components/TimerDrawable.java org/telegram/ui/Components/TranscribeButton.java org/telegram/ui/Components/TranslateAlert2.java org/telegram/ui/Components/UndoView.java org/telegram/ui/Components/VideoPlayer.java org/telegram/ui/Components/VideoPlayerSeekBar.java org/telegram/ui/Components/VideoSeekPreviewImage.java org/telegram/ui/Components/VideoTimelinePlayView.java org/telegram/ui/Components/VideoTimelineView.java org/telegram/ui/Components/WallpaperUpdater.java org/telegram/ui/Components/WebPlayerView.java org/telegram/ui/Components/spoilers/SpoilerEffect2.java org/telegram/ui/Components/voip/VoIPHelper.java org/telegram/ui/Components/voip/VoIPPiPView.java org/telegram/ui/ContactsActivity.java org/telegram/ui/ContentPreviewViewer.java org/telegram/ui/CountrySelectActivity.java org/telegram/ui/DialogsActivity.java org/telegram/ui/EditWidgetActivity.java org/telegram/ui/EmojiAnimationsOverlay.java org/telegram/ui/ExternalActionActivity.java org/telegram/ui/FilterChatlistActivity.java org/telegram/ui/FilterCreateActivity.java org/telegram/ui/FilteredSearchView.java org/telegram/ui/FiltersSetupActivity.java org/telegram/ui/GroupCallActivity.java org/telegram/ui/GroupCreateActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/telegram/ui/GroupCreateFinalActivity.java org/telegram/ui/GroupInviteActivity.java org/telegram/ui/GroupStickersActivity.java org/telegram/ui/IdenticonActivity.java org/telegram/ui/IntroActivity.java org/telegram/ui/InviteContactsActivity.java org/telegram/ui/LanguageSelectActivity.java org/telegram/ui/LaunchActivity.java org/telegram/ui/LinkEditActivity.java org/telegram/ui/LocationActivity.java org/telegram/ui/LoginActivity.java org/telegram/ui/ManageLinksActivity.java org/telegram/ui/MessageSendPreview.java org/telegram/ui/NewContactBottomSheet.java org/telegram/ui/NotificationsCustomSettingsActivity.java org/telegram/ui/NotificationsSettingsActivity.java org/telegram/ui/NotificationsSoundActivity.java org/telegram/ui/PasscodeActivity.java org/telegram/ui/PassportActivity.java org/telegram/ui/PaymentFormActivity.java org/telegram/ui/PhotoCropActivity.java org/telegram/ui/PhotoViewer.java org/telegram/ui/PollCreateActivity.java org/telegram/ui/PopupNotificationActivity.java org/telegram/ui/PremiumPreviewFragment.java org/telegram/ui/PrivacySettingsActivity.java org/telegram/ui/ProfileActivity.java org/telegram/ui/ProfileBirthdayEffect.java org/telegram/ui/ProfileNotificationsActivity.java org/telegram/ui/QrActivity.java org/telegram/ui/RestrictedLanguagesSelectActivity.java org/telegram/ui/SecretMediaViewer.java org/telegram/ui/SelectAnimatedEmojiDialog.java org/telegram/ui/SessionsActivity.java org/telegram/ui/ShareActivity.java org/telegram/ui/Stars/BotStarsActivity.java org/telegram/ui/Stars/StarsController.java org/telegram/ui/Stars/StarsIntroActivity.java org/telegram/ui/StickersActivity.java org/telegram/ui/Stories/LivePlayer.java org/telegram/ui/Stories/PeerStoriesView.java org/telegram/ui/Stories/SelfStoryViewsPage.java org/telegram/ui/Stories/SelfStoryViewsView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/telegram/ui/Stories/StoriesController.java org/telegram/ui/Stories/StoriesStorage.java org/telegram/ui/Stories/StoriesViewPager.java org/telegram/ui/Stories/StoryCaptionView.java org/telegram/ui/Stories/StoryViewer.java org/telegram/ui/Stories/recorder/CaptionContainerView.java org/telegram/ui/Stories/recorder/DownloadButton.java org/telegram/ui/Stories/recorder/DraftsController.java org/telegram/ui/Stories/recorder/DualCameraView.java org/telegram/ui/Stories/recorder/EmojiBottomSheet.java org/telegram/ui/Stories/recorder/PaintView.java org/telegram/ui/Stories/recorder/ScannedLinkPreview.java org/telegram/ui/Stories/recorder/StoryEntry.java org/telegram/ui/Stories/recorder/StoryLinkSheet.java org/telegram/ui/Stories/recorder/StoryPrivacySelector.java org/telegram/ui/Stories/recorder/StoryRecorder.java org/telegram/ui/Stories/recorder/StoryUploadingService.java org/telegram/ui/Stories/recorder/TimelineView.java org/telegram/ui/Stories/recorder/Weather.java org/telegram/ui/TON/TONIntroActivity.java org/telegram/ui/ThemeActivity.java org/telegram/ui/ThemePreviewActivity.java org/telegram/ui/ThemeSetUrlActivity.java org/telegram/ui/TopicsFragment.java org/telegram/ui/TwoStepVerificationActivity.java org/telegram/ui/TwoStepVerificationSetupActivity.java org/telegram/ui/VoIPFragment.java org/telegram/ui/VoIPPermissionActivity.java org/telegram/ui/WallpapersListActivity.java org/telegram/ui/WebviewActivity.java org/telegram/ui/bots/BotBiometry.java org/telegram/ui/bots/BotDownloads.java org/telegram/ui/bots/BotLocation.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/telegram/ui/bots/BotLocation.java org/telegram/ui/bots/BotShareSheet.java org/telegram/ui/bots/BotStorage.java org/telegram/ui/bots/BotWebViewSheet.java org/telegram/ui/bots/WebViewRequestProps.java org/telegram/ui/web/AddressBarList.java org/telegram/ui/web/BotWebViewContainer.java org/telegram/ui/web/BrowserHistory.java org/telegram/ui/web/HttpGetFileTask.java org/telegram/ui/web/RestrictedDomainsList.java org/telegram/ui/web/SearchEngine.java org/telegram/ui/web/WebBrowserSettings.java org/telegram/ui/web/WebInstantView.java org/telegram/ui/web/WebMetadataCache.java org/webrtc/AndroidVideoDecoder.java org/webrtc/EglRenderer.java org/webrtc/GlGenericDrawer.java org/webrtc/ScreenCapturerAndroid.java org/webrtc/YuvConverter.java org/webrtc/audio/WebRtcAudioTrack.java org/webrtc/voiceengine/WebRtcAudioRecord.java org/webrtc/voiceengine/WebRtcAudioTrack.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/microsoft/appcenter/channel/DefaultChannel.java org/telegram/messenger/BuildVars.java org/telegram/messenger/ImageLoader.java org/telegram/messenger/ImageReceiver.java org/telegram/messenger/MediaDataController.java org/telegram/messenger/PushListenerController.java org/telegram/messenger/voip/Instance.java org/telegram/ui/Adapters/MentionsAdapter.java org/telegram/ui/ArticleViewer.java org/telegram/ui/ChannelCreateActivity.java org/telegram/ui/ChatEditTypeActivity.java org/telegram/ui/Components/Reactions/ReactionsLayoutInBubble.java org/telegram/ui/DataAutoDownloadActivity.java org/telegram/ui/PremiumPreviewFragment.java org/telegram/ui/QrActivity.java org/telegram/ui/Stories/recorder/DualCameraView.java org/telegram/ui/TodoItemMenu.java org/telegram/ui/TopicsFragment.java
3	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	org/telegram/ui/ArticleViewer.java org/telegram/ui/Components/EmbedBottomSheet.java org/telegram/ui/Components/PhotoViewerWebView.java org/telegram/ui/Components/WebPlayerView.java org/telegram/ui/PaymentFormActivity.java org/telegram/ui/WebviewActivity.java org/telegram/ui/web/BotWebViewContainer.java org/telegram/ui/web/WebInstantView.java org/telegram/ui/web/WebMetadataCache.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	org/telegram/messenger/AndroidUtilities.java org/telegram/messenger/EmuDetector.java org/telegram/messenger/FilesMigrationService.java org/telegram/messenger/ImageLoader.java org/telegram/messenger/MediaController.java org/telegram/messenger/SharedConfig.java org/telegram/messenger/voip/VoIPController.java org/telegram/ui/Components/ChatAttachAlertDocumentLayout.java org/telegram/ui/Components/voip/VoIPHelper.java
5	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	org/telegram/ui/ProxySettingsActivity.java
6	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	org/telegram/messenger/BuildConfig.java
7	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	org/telegram/messenger/AndroidUtilities.java org/telegram/ui/ChangeUsernameActivity.java org/telegram/ui/ChatActivity.java org/telegram/ui/Components/EmbedBottomSheet.java org/telegram/ui/Components/InviteMembersBottomSheet.java org/telegram/ui/Components/LinkActionView.java org/telegram/ui/Components/PhonebookShareAlert.java org/telegram/ui/Components/ShareAlert.java org/telegram/ui/GroupInviteActivity.java org/telegram/ui/ManageLinksActivity.java org/telegram/ui/PrivacyControlActivity.java org/telegram/ui/ProfileActivity.java org/telegram/ui/SessionBottomSheet.java org/telegram/ui/StickersActivity.java org/telegram/ui/ThemeSetUrlActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/carrotsearch/randomizedtesting/Xoroshiro128PlusRandom.java com/microsoft/appcenter/http/HttpClientRetryer.java j$/util/concurrent/ThreadLocalRandom.java org/telegram/messenger/Utilities.java org/telegram/ui/Components/AudioVisualizerDrawable.java org/telegram/ui/Components/AvatarsDrawable.java org/telegram/ui/Components/BlobDrawable.java org/telegram/ui/Components/CircleBezierDrawable.java org/telegram/ui/Components/FlickerLoadingView.java org/telegram/ui/Components/GroupCallPipButton.java org/telegram/ui/Components/LineBlobDrawable.java org/telegram/ui/Components/MotionBackgroundDrawable.java org/telegram/ui/Components/Reactions/ReactionsEffectOverlay.java org/telegram/ui/Components/SharedMediaFastScrollTooltip.java org/telegram/ui/EmojiAnimationsOverlay.java org/telegram/ui/Stars/BagRandomizer.java
9	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/utils/storage/DatabaseManager.java
10	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	fi/iki/elonen/NanoHTTPD.java org/telegram/messenger/EmuDetector.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	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	org/telegram/messenger/FileUploadOperation.java org/telegram/messenger/MessagesController.java org/telegram/messenger/Utilities.java
12	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	org/telegram/ui/Components/Paint/Slice.java
13	This App uses SQL Cipher. Ensure that secrets are not hardcoded in code.	info	OWASP MASVS: MSTG-CRYPTO-1	com/microsoft/appcenter/utils/storage/DatabaseManager.java
14	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	org/telegram/messenger/Utilities.java org/telegram/ui/PassportActivity.java
15	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	org/telegram/ui/bots/BotBiometry.java
16	This App uses SafetyNet API.	secure	OWASP MASVS: MSTG-RESILIENCE-7	org/telegram/ui/LoginActivity.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	x86/liblanguage_id_l2c_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	x86/libtmessages.49.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__FD_ISSET_chk', '__FD_SET_chk', '__FD_CLR_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	armeabi-v7a/liblanguage_id_l2c_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	armeabi-v7a/libtmessages.49.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__FD_ISSET_chk', '__FD_SET_chk', '__FD_CLR_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/liblanguage_id_l2c_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	arm64-v8a/libtmessages.49.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__FD_SET_chk', '__memcpy_chk', '__memset_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__vsnprintf_chk', '__memmove_chk', '__fgets_chk', '__read_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	x86_64/liblanguage_id_l2c_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86_64/libtmessages.49.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__read_chk', '__fgets_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__FD_CLR_chk', '__strlen_chk', '__memcpy_chk', '__strchr_chk', '__vsnprintf_chk', '__memset_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	x86/liblanguage_id_l2c_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	x86/libtmessages.49.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__FD_ISSET_chk', '__FD_SET_chk', '__FD_CLR_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	armeabi-v7a/liblanguage_id_l2c_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	armeabi-v7a/libtmessages.49.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__FD_ISSET_chk', '__FD_SET_chk', '__FD_CLR_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	arm64-v8a/liblanguage_id_l2c_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	arm64-v8a/libtmessages.49.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__FD_SET_chk', '__memcpy_chk', '__memset_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__vsnprintf_chk', '__memmove_chk', '__fgets_chk', '__read_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	x86_64/liblanguage_id_l2c_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	x86_64/libtmessages.49.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__read_chk', '__fgets_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__FD_CLR_chk', '__strlen_chk', '__memcpy_chk', '__strchr_chk', '__vsnprintf_chk', '__memset_chk', '__memmove_chk']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/microsoft/appcenter/distribute/BrowserUtils.java com/microsoft/appcenter/distribute/Distribute.java com/microsoft/appcenter/distribute/DistributeUtils.java org/telegram/messenger/AndroidUtilities.java org/telegram/messenger/BillingController.java org/telegram/messenger/ChatsWidgetProvider.java org/telegram/messenger/ContactsWidgetProvider.java org/telegram/messenger/FeedWidgetProvider.java org/telegram/messenger/ImageLoader.java org/telegram/messenger/MediaController.java org/telegram/messenger/MusicBrowserService.java org/telegram/messenger/MusicPlayerService.java org/telegram/messenger/NotificationBadge.java org/telegram/messenger/NotificationsController.java org/telegram/messenger/browser/Browser.java org/telegram/messenger/support/customtabsclient/shared/CustomTabsHelper.java org/telegram/messenger/voip/VoIPPreNotificationService.java org/telegram/messenger/voip/VoIPService.java org/telegram/ui/ActionIntroActivity.java org/telegram/ui/ArticleViewer.java org/telegram/ui/BasePermissionsActivity.java org/telegram/ui/CameraScanActivity.java org/telegram/ui/ChannelAdminLogActivity.java org/telegram/ui/ChatActivity.java org/telegram/ui/Components/AlertsCreator.java org/telegram/ui/Components/EmbedBottomSheet.java org/telegram/ui/Components/PermissionRequest.java org/telegram/ui/Components/PhonebookShareAlert.java org/telegram/ui/Components/PhotoViewerWebView.java org/telegram/ui/Components/Premium/PremiumNotAvailableBottomSheet.java org/telegram/ui/DialogsActivity.java org/telegram/ui/InviteContactsActivity.java org/telegram/ui/LaunchActivity.java org/telegram/ui/LocationActivity.java org/telegram/ui/LoginActivity.java org/telegram/ui/NotificationsSettingsActivity.java org/telegram/ui/NotificationsSoundActivity.java org/telegram/ui/PassportActivity.java org/telegram/ui/PaymentFormActivity.java org/telegram/ui/PhotoViewer.java

RULE ID	BEHAVIOUR	LABEL	FILES
			org/telegram/ui/PopupNotificationActivity.java org/telegram/ui/PremiumPreviewFragment.java org/telegram/ui/ProfileActivity.java org/telegram/ui/ProfileNotificationsActivity.java
			org/telegram/ui/QrActivity.java org/telegram/ui/SessionsActivity.java org/telegram/ui/Stories/PeerStoriesView.java org/telegram/ui/Stories/recorder/StoryRecorder.java org/telegram/ui/WebviewActivity.java org/telegram/ui/bots/BotLocation.java org/telegram/ui/web/BotWebViewContainer.java
			com/microsoft/appcenter/crashes/Crashes.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java com/microsoft/appcenter/utils/storage/FileManager.java org/telegram/messenger/AndroidUtilities.java org/telegram/messenger/AutoDeleteMediaTask.java org/telegram/messenger/BetaUpdaterController.java org/telegram/messenger/ChatThemeController.java org/telegram/messenger/DatabaseMigrationHelper.java org/telegram/messenger/FileLoader.java org/telegram/messenger/FileLog.java org/telegram/messenger/FilePathDatabase.java org/telegram/messenger/FilesMigrationService.java org/telegram/messenger/ImageLoader.java org/telegram/messenger/LocaleController.java org/telegram/messenger/MediaController.java org/telegram/messenger/MessageObject.java org/telegram/messenger/MessagesController.java org/telegram/messenger/MusicPlayerService.java org/telegram/messenger/NativeLoader.java org/telegram/messenger/NotificationsController.java org/telegram/messenger/SecretChatHelper.java org/telegram/messenger/SendMessagesHelper.java org/telegram/messenger/SharedConfig.java org/telegram/messenger/VideoEditedInfo.java org/telegram/messenger/audioinfo/AudioInfo.java org/telegram/messenger/audioinfo/OtherAudioInfo.java org/telegram/messenger/camera/CameraController.java org/telegram/messenger/chromecast/ChromecastControllerState.java org/telegram/messenger/video/VideoFramesRewinder.java org/telegram/messenger/video/WebmEncoder.java org/telegram/messenger/voip/VoIPController.java org/telegram/messenger/voip/VoIPDebugToSend.java

RULE ID	BEHAVIOUR	LABEL	FILES
			org/telegram/messenger/voip/VoIPService.java org/telegram/ui/ActionBar/EmojiThemes.java org/telegram/ui/ActionBar/Theme.java org/telegram/ui/CacheControlActivity.java
00022	Open a file from given absolute path of the file	file	org/telegram/ui/CachedMediaLayout.java org/telegram/ui/Cells/ContextLinkCell.java org/telegram/ui/Cells/PhotoAttachCameraCell.java org/telegram/ui/Cells/ThemesHorizontalListCell.java org/telegram/ui/Cells/WallpaperCell.java org/telegram/ui/ChannelColorActivity.java org/telegram/ui/ChatActivity.java org/telegram/ui/Components/AnimatedFileDrawable.java org/telegram/ui/Components/ChatActivityEnterView.java org/telegram/ui/Components/ChatAttachAlert.java org/telegram/ui/Components/ChatAttachAlertDocumentLayout.java org/telegram/ui/Components/ChatAttachAlertLocationLayout.java org/telegram/ui/Components/ChatAttachAlertPhotoLayout.java org/telegram/ui/Components/ChatThemeBottomSheet.java org/telegram/ui/Components/Crop/CropView.java org/telegram/ui/Components/ImageUpdater.java org/telegram/ui/Components/InstantCameraView.java org/telegram/ui/Components/Paint/Views/LPhotoPaintView.java org/telegram/ui/Components/Paint/Views/PhotoView.java org/telegram/ui/Components/Paint/Views/StickerMakerView.java org/telegram/ui/Components/RLottieDrawable.java org/telegram/ui/Components/StickersAlert.java org/telegram/ui/Components/ThemePreviewDrawable.java org/telegram/ui/Components/VideoSeekPreviewImage.java org/telegram/ui/Components/WallpaperUpdater.java org/telegram/ui/Components/voip/PrivateVideoPreviewDialog.java org/telegram/ui/Components/voip/PrivateVideoPreviewDialogNew.java org/telegram/ui/Components/voip/VoIPHelper.java org/telegram/ui/Components/voip/VoIPTextureView.java org/telegram/ui/DataSettingsActivity.java org/telegram/ui/LaunchActivity.java org/telegram/ui/PassportActivity.java org/telegram/ui/PhotoViewer.java org/telegram/ui/ProfileActivity.java org/telegram/ui/SecretMediaViewer.java org/telegram/ui/Stories/StoriesController.java org/telegram/ui/Stories/recorder/DownloadButton.java org/telegram/ui/Stories/recorder/DraftsController.java org/telegram/ui/Stories/recorder/PaintView.java org/telegram/ui/Stories/recorder/PreviewView.java

RULE ID	BEHAVIOUR	LABEL	FILES
			org/telegram/ui/Stories/recorder/StoryEntry.java org/telegram/ui/Stories/recorder/StoryRecorder.java org/telegram/ui/ThemePreviewActivity.java org/telegram/ui/bots/BotDownloads.java
			org/telegram/ui/bots/BotShareSheet.java org/telegram/ui/web/BotWebViewContainer.java org/telegram/ui/web/WebInstantView.java
00013	Read file and put it into a stream	file	com/microsoft/appcenter/utils/storage/FileManager.java org/telegram/messenger/AndroidUtilities.java org/telegram/messenger/ChatThemeController.java org/telegram/messenger/EmuDetector.java org/telegram/messenger/EmuInputDevicesDetector.java org/telegram/messenger/FileLoadOperation.java org/telegram/messenger/ImageLoader.java org/telegram/messenger/LocaleController.java org/telegram/messenger/MediaController.java org/telegram/messenger/SendMessagesHelper.java org/telegram/messenger/SvgHelper.java org/telegram/messenger/Utilities.java org/telegram/messenger/audioinfo/AudioInfo.java org/telegram/messenger/chromecast/ChromecastFileServer.java org/telegram/messenger/secretmedia/EncryptedFileInputStream.java org/telegram/messenger/voip/VoIPService.java org/telegram/tgnet/SerializedData.java org/telegram/ui/ActionBar/Theme.java org/telegram/ui/Cells/ThemesHorizontalListCell.java org/telegram/ui/ChannelColorActivity.java org/telegram/ui/Components/ChatThemeBottomSheet.java org/telegram/ui/Components/Paint/Slice.java org/telegram/ui/ProfileActivity.java org/telegram/ui/bots/BotStorage.java org/telegram/ui/web/MHTML.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	org/telegram/messenger/AndroidUtilities.java org/telegram/messenger/SendMessagesHelper.java org/telegram/ui/ArticleViewer.java org/telegram/ui/CacheControlActivity.java org/telegram/ui/ChannelAdminLogActivity.java org/telegram/ui/ChatActivity.java org/telegram/ui/Components/AudioPlayerAlert.java org/telegram/ui/Components/ChatThemeBottomSheet.java org/telegram/ui/Components/ImageUpdater.java org/telegram/ui/LaunchActivity.java org/telegram/ui/NotificationsSoundActivity.java org/telegram/ui/PassportActivity.java org/telegram/ui/PhotoCropActivity.java org/telegram/ui/PhotoViewer.java org/telegram/ui/ProfileActivity.java org/telegram/ui/SecretVoicePlayer.java org/telegram/ui/Stories/PeerStoriesView.java org/telegram/ui/Stories/recorder/PaintView.java org/telegram/ui/ThemePreviewActivity.java org/telegram/ui/bots/BotShareSheet.java
00065	Get the country code of the SIM card provider	collection	org/telegram/messenger/LocaleController.java org/telegram/ui/ChatActivity.java org/telegram/ui/NewContactBottomSheet.java org/telegram/ui/PassportActivity.java org/telegram/ui/PaymentFormActivity.java
00112	Get the date of the calendar event	collection calendar	org/telegram/messenger/LocaleController.java org/telegram/ui/Components/AlertsCreator.java
00003	Put the compressed bitmap data into JSON object	camera	org/telegram/messenger/ImageLoader.java org/telegram/messenger/SendMessagesHelper.java org/telegram/ui/ActionBar/Theme.java org/telegram/ui/web/BotWebViewContainer.java

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	org/telegram/messenger/ImageLoader.java org/telegram/messenger/SendMessagesHelper.java org/telegram/messenger/voip/VoIPService.java org/telegram/ui/ActionBar/Theme.java org/telegram/ui/bots/BotStorage.java
00005	Get absolute path of file and put it to JSON object	file	com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java org/telegram/messenger/ImageLoader.java org/telegram/messenger/SendMessagesHelper.java org/telegram/messenger/SharedConfig.java org/telegram/messenger/voip/VoIPService.java org/telegram/ui/ActionBar/Theme.java org/telegram/ui/PassportActivity.java org/telegram/ui/bots/BotDownloads.java org/telegram/ui/web/BotWebViewContainer.java org/telegram/ui/web/WebInstantView.java
00072	Write HTTP input stream into a file	command network file	org/telegram/messenger/ImageLoader.java org/telegram/ui/web/BotWebViewContainer.java org/telegram/ui/web/HttpGetFileTask.java
00004	Get filename and put it to JSON object	file collection	com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java org/telegram/messenger/ImageLoader.java org/telegram/messenger/SendMessagesHelper.java org/telegram/messenger/SharedConfig.java org/telegram/messenger/voip/VoIPService.java org/telegram/ui/ActionBar/Theme.java org/telegram/ui/ArticleViewer.java org/telegram/ui/bots/BotDownloads.java org/telegram/ui/bots/BotStorage.java org/telegram/ui/web/BotWebViewContainer.java
00123	Save the response to JSON after connecting to the remote server	network command	org/telegram/messenger/ImageLoader.java org/telegram/ui/Components/WebPlayerView.java org/telegram/ui/web/BotWebViewContainer.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/stripe/android/net/StripeApiHandler.java org/telegram/messenger/ImageLoader.java org/telegram/ui/Components/PhotoViewerWebView.java org/telegram/ui/Components/WebPlayerView.java org/telegram/ui/PaymentFormActivity.java org/telegram/ui/bots/BotDownloads.java org/telegram/ui/web/BotWebViewContainer.java org/telegram/ui/web/HttpGetBitmapTask.java org/telegram/ui/web/HttpGetFileTask.java org/telegram/ui/web/HttpGetTask.java
00163	Create new Socket and connecting to it	socket	org/telegram/messenger/ImageLoader.java org/telegram/tgnet/ConnectionsManager.java org/telegram/ui/Components/WebPlayerView.java
00030	Connect to the remote server through the given URL	network	org/telegram/messenger/ImageLoader.java org/telegram/ui/Components/WebPlayerView.java org/telegram/ui/web/BotWebViewContainer.java
00109	Connect to a URL and get the response code	network command	com/stripe/android/net/StripeApiHandler.java org/telegram/messenger/ImageLoader.java org/telegram/ui/Components/PhotoViewerWebView.java org/telegram/ui/Components/WebPlayerView.java org/telegram/ui/PaymentFormActivity.java org/telegram/ui/bots/BotDownloads.java org/telegram/ui/web/BotWebViewContainer.java org/telegram/ui/web/HttpGetBitmapTask.java org/telegram/ui/web/HttpGetFileTask.java org/telegram/ui/web/HttpGetTask.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	org/telegram/messenger/ImageLoader.java org/telegram/messenger/SendMessagesHelper.java org/telegram/messenger/camera/CameraController.java org/telegram/messenger/utils/BitmapsCache.java

RULE ID	BEHAVIOUR	LABEL	FILES
00094	Connect to a URL and read data from it	command network	org/telegram/messenger/ImageLoader.java org/telegram/tgnet/ConnectionsManager.java org/telegram/ui/Components/PhotoViewerWebView.java org/telegram/ui/Components/WebPlayerView.java org/telegram/ui/web/HttpGetFileTask.java
00108	Read the input stream from given URL	network command	org/telegram/messenger/ImageLoader.java org/telegram/ui/Components/PhotoViewerWebView.java org/telegram/ui/Components/TranslateAlert2.java org/telegram/ui/Components/WebPlayerView.java org/telegram/ui/web/HttpGetFileTask.java
00137	Get last known location of the device	location collection	org/telegram/messenger/LocationController.java org/telegram/messenger/SendMessagesHelper.java org/telegram/ui/Components/ChatAttachAlertLocationLayout.java org/telegram/ui/LocationActivity.java org/telegram/ui/ThemeActivity.java
00115	Get last known location of the device	collection location	org/telegram/messenger/LocationController.java org/telegram/messenger/SendMessagesHelper.java org/telegram/ui/Components/ChatAttachAlertLocationLayout.java org/telegram/ui/LocationActivity.java org/telegram/ui/Stories/recorder/Weather.java org/telegram/ui/ThemeActivity.java org/telegram/ui/bots/BotLocation.java
00189	Get the content of a SMS message	sms	org/telegram/messenger/ContactsController.java org/telegram/messenger/MediaController.java org/telegram/messenger/NotificationBadge.java
00188	Get the address of a SMS message	sms	org/telegram/messenger/ContactsController.java org/telegram/messenger/MediaController.java org/telegram/messenger/NotificationBadge.java

RULE ID	BEHAVIOUR	LABEL	FILES
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	org/telegram/messenger/ContactsController.java org/telegram/messenger/MediaController.java org/telegram/messenger/NotificationBadge.java
00191	Get messages in the SMS inbox	sms	org/telegram/messenger/ContactsController.java org/telegram/messenger/MediaController.java org/telegram/messenger/NotificationBadge.java org/telegram/ui/bots/BotDownloads.java
00200	Query data from the contact list	collection contact	org/telegram/messenger/ContactsController.java org/telegram/messenger/MediaController.java org/telegram/messenger/NotificationBadge.java
00187	Query a URI and check the result	collection sms calllog calendar	org/telegram/messenger/ContactsController.java org/telegram/messenger/MediaController.java org/telegram/messenger/NotificationBadge.java
00201	Query data from the call log	collection calllog	org/telegram/messenger/ContactsController.java org/telegram/messenger/MediaController.java org/telegram/messenger/NotificationBadge.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	org/telegram/messenger/ContactsController.java org/telegram/messenger/MediaController.java org/telegram/messenger/NotificationBadge.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/microsoft/appcenter/distribute/Distribute.java org/telegram/messenger/AndroidUtilities.java org/telegram/messenger/BillingController.java org/telegram/messenger/ChatsWidgetProvider.java org/telegram/messenger/ContactsWidgetProvider.java org/telegram/messenger/FeedWidgetProvider.java org/telegram/messenger/MusicBrowserService.java org/telegram/messenger/NotificationBadge.java org/telegram/messenger/browser/Browser.java org/telegram/messenger/voip/VoIPPreNotificationService.java org/telegram/ui/ActionIntroActivity.java org/telegram/ui/ArticleViewer.java org/telegram/ui/Cells/ChatMessageCell.java org/telegram/ui/ChatActivity.java org/telegram/ui/Components/AlertsCreator.java org/telegram/ui/DialogsActivity.java org/telegram/ui/LaunchActivity.java org/telegram/ui/LocationActivity.java org/telegram/ui/LoginActivity.java org/telegram/ui/PassportActivity.java org/telegram/ui/PopupNotificationActivity.java org/telegram/ui/ProfileActivity.java org/telegram/ui/QrActivity.java org/telegram/ui/SessionsActivity.java org/telegram/ui/Stories/recorder/StoryRecorder.java org/telegram/ui/WebviewActivity.java org/telegram/ui/bots/BotLocation.java org/telegram/ui/web/BotWebViewContainer.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/microsoft/appcenter/distribute/Distribute.java org/telegram/messenger/AndroidUtilities.java org/telegram/messenger/ChatsWidgetProvider.java org/telegram/messenger/ContactsWidgetProvider.java org/telegram/messenger/FeedWidgetProvider.java org/telegram/messenger/MusicPlayerService.java org/telegram/messenger/NotificationsController.java org/telegram/ui/ActionIntroActivity.java org/telegram/ui/BasePermissionsActivity.java org/telegram/ui/ChatActivity.java org/telegram/ui/Components/AlertsCreator.java org/telegram/ui/Components/PermissionRequest.java org/telegram/ui/DialogsActivity.java org/telegram/ui/LocationActivity.java org/telegram/ui/LoginActivity.java org/telegram/ui/PassportActivity.java org/telegram/ui/PhotoViewer.java org/telegram/ui/PopupNotificationActivity.java org/telegram/ui/PremiumPreviewFragment.java org/telegram/ui/ProfileActivity.java org/telegram/ui/ProfileNotificationsActivity.java org/telegram/ui/QrActivity.java org/telegram/ui/SessionsActivity.java org/telegram/ui/Stories/recorder/StoryRecorder.java org/telegram/ui/bots/BotLocation.java
00096	Connect to a URL and set request method	command network	com/stripe/android/net/StripeApiHandler.java org/telegram/ui/Components/PhotoViewerWebView.java org/telegram/ui/PaymentFormActivity.java org/telegram/ui/bots/BotDownloads.java org/telegram/ui/web/BotWebViewContainer.java org/telegram/ui/web/HttpGetBitmapTask.java org/telegram/ui/web/HttpGetFileTask.java org/telegram/ui/web/HttpGetTask.java

RULE ID	BEHAVIOUR	LABEL	FILES
00038	Query the phone number	collection	org/telegram/messenger/EmuDetector.java org/telegram/ui/LoginActivity.java org/telegram/ui/PassportActivity.java org/telegram/ui/PaymentFormActivity.java
00151	Send phone number over Internet	phone privacy	org/telegram/ui/PaymentFormActivity.java
00024	Write file after Base64 decoding	reflection file	org/telegram/messenger/camera/CameraController.java org/telegram/ui/ActionBar/Theme.java
00012	Read data and put it into a buffer stream	file	org/telegram/messenger/AndroidUtilities.java org/telegram/messenger/audioinfo/AudioInfo.java org/telegram/messenger/chromecast/ChromecastFileServer.java org/telegram/ui/ProfileActivity.java org/telegram/ui/web/MHTML.java
00064	Monitor incoming call status	control	org/telegram/messenger/voip/VoIPService.java
00102	Set the phone speaker on	command	org/telegram/messenger/MediaController.java org/telegram/messenger/voip/VoIPService.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	org/telegram/messenger/ContactsController.java org/telegram/messenger/MediaController.java
00053	Monitor data identified by a given content URI changes(SMS, MMS, etc.)	sms	org/telegram/messenger/ContactsController.java org/telegram/messenger/MediaController.java
00204	Get the default ringtone	collection	org/telegram/ui/NotificationsSettingsActivity.java org/telegram/ui/NotificationsSoundActivity.java org/telegram/ui/ProfileNotificationsActivity.java
00192	Get messages in the SMS inbox	sms	com/microsoft/appcenter/distribute/download/manager/DownloadManagerReleaseDownloader.java org/telegram/messenger/AndroidUtilities.java

RULE ID	BEHAVIOUR	LABEL	FILES
00104	Check if the given path is directory	file	org/telegram/messenger/AndroidUtilities.java org/telegram/ui/CacheControlActivity.java org/telegram/ui/ProfileActivity.java
00146	Get the network operator name and IMSI	telephony collection	org/telegram/messenger/EmuDetector.java
00078	Get the network operator name	collection telephony	com/microsoft/appcenter/utils/DeviceInfoHelper.java org/telegram/messenger/EmuDetector.java
00117	Get the IMSI and network operator name	telephony collection	org/telegram/messenger/EmuDetector.java
00033	Query the IMEI number	collection	org/telegram/messenger/EmuDetector.java
00067	Query the IMSI number	collection	org/telegram/messenger/EmuDetector.java
00075	Get location of the device	collection location	org/telegram/ui/Components/ChatAttachAlertLocationLayout.java org/telegram/ui/LocationActivity.java org/telegram/ui/Stories/recorder/Weather.java org/telegram/ui/ThemeActivity.java org/telegram/ui/bots/BotLocation.java
00199	Stop recording and release recording resources	record	org/telegram/messenger/camera/CameraController.java org/webrtc/CameraCapturer.java
00202	Make a phone call	control	org/telegram/messenger/NotificationsController.java org/telegram/ui/ChatActivity.java org/telegram/ui/PhotoViewer.java org/telegram/ui/PremiumPreviewFragment.java org/telegram/ui/ProfileActivity.java
00203	Put a phone number into an intent	control	org/telegram/messenger/NotificationsController.java org/telegram/ui/ChatActivity.java org/telegram/ui/PhotoViewer.java org/telegram/ui/PremiumPreviewFragment.java org/telegram/ui/ProfileActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00056	Modify voice volume	control	org/telegram/ui/CastSync.java org/telegram/ui/PhotoViewer.java org/telegram/ui/Stories/StoriesVolumeControl.java org/webrtc/audio/WebRtcAudioTrack.java org/webrtc/voiceengine/WebRtcAudioTrack.java
00054	Install other APKs from file	reflection	org/telegram/messenger/AndroidUtilities.java org/telegram/messenger/ApplicationLoaderImpl.java org/telegram/ui/ChannelAdminLogActivity.java org/telegram/ui/ChatActivity.java
00183	Get current camera parameters and change the setting.	camera	org/telegram/messenger/camera/CameraController.java org/telegram/messenger/camera/CameraSession.java org/webrtc/Camera1Session.java
00018	Get JSON object prepared and fill in location info	location collection	org/telegram/messenger/SendMessagesHelper.java org/telegram/ui/bots/BotLocation.java
00113	Get location and put it into JSON	collection location	org/telegram/messenger/SendMessagesHelper.java org/telegram/ui/bots/BotLocation.java
00016	Get location info of the device and put it to JSON object	location collection	org/telegram/messenger/SendMessagesHelper.java org/telegram/ui/bots/BotLocation.java
00009	Put data in cursor to JSON object	file	org/telegram/messenger/SendMessagesHelper.java org/telegram/ui/bots/BotDownloads.java
00039	Start a web server	control network	fi/iki/elonen/NanoHTTPD.java
00208	Capture the contents of the device screen	collection screen	org/webrtc/ScreenCapturerAndroid.java
00121	Create a directory	file command	org/telegram/messenger/AndroidUtilities.java org/telegram/ui/ChannelAdminLogActivity.java org/telegram/ui/ChatActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00132	Query The ISO country code	telephony collection	com/microsoft/appcenter/utils/DeviceInfoHelper.java
00079	Hide the current app's icon	evasion	org/telegram/ui/LauncherIconController.java
00209	Get pixels from the latest rendered image	collection	org/telegram/messenger/camera/Camera2Session.java
00092	Send broadcast	command	org/telegram/messenger/AndroidUtilities.java
00002	Open the camera and take picture	camera	org/telegram/messenger/camera/CameraController.java
00195	Set the output path of the recorded file	record file	org/telegram/messenger/camera/CameraController.java
00198	Initialize the recorder and start recording	record	org/telegram/messenger/camera/CameraController.java
00007	Use absolute path of directory for the output media file path	file	org/telegram/messenger/camera/CameraController.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://tmessages2.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/760348033671/namespaces/firebase:fetch?key=AIzaSyA-t0jLPjUt2FxrA8VPK2EiYHcYcboIR6k. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	17/25	android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.INTERNET, android.permission.RECORD_AUDIO, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE, android.permission.GET_ACCOUNTS, android.permission.READ_CONTACTS, android.permission.VIBRATE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.READ_PHONE_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.CAMERA, android.permission.REQUEST_INSTALL_PACKAGES, android.permission.WRITE_EXTERNAL_STORAGE
Other Common Permissions	8/44	com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.WRITE_CONTACTS, android.permission.AUTHENTICATE_ACCOUNTS, com.android.launcher.permission.INSTALL_SHORTCUT, android.permission.BLUETOOTH, android.permission.ACCESS_BACKGROUND_LOCATION

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

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
fragment.com	malware **URL:** fragment.com **IP:** N/A **Description:** Malicious Domain tagged by Maltrail	**IP:** 104.20.26.203 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
getdesktop.telegram.org	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
duckduckgo.com	ok	**IP:** 52.250.42.157 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
youtube.googleapis.com	ok	**IP:** 142.251.34.202 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
translate.googleapis.com	ok	**IP:** 142.250.217.74 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
instagram.com	ok	**IP:** 57.144.216.34 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map
ads.telegram.org	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
maps.googleapis.com	ok	**IP:** 142.251.33.74 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
crbug.com	ok	**IP:** 216.239.32.29 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.ietf.org	ok	**IP:** 104.16.44.99 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
desktop.telegram.org	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
mozilla.cloudflare-dns.com	ok	**IP:** 172.64.41.4 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
webrtc.googlesource.com	ok	**IP:** 74.125.142.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
static-maps.yandex.ru	ok	**IP:** 213.180.204.41 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
www.bing.com	ok	**IP:** 207.194.199.137 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
www.instagram.com	ok	**IP:** 57.144.216.34 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.example.com	ok	**IP:** 23.218.239.25 **Country:** Brazil **Region:** Sao Paulo **City:** Sao Paulo **Latitude:** -23.547501 **Longitude:** -46.636108 **View:** Google Map
api.twitch.tv	ok	**IP:** 18.172.185.6 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
install.appcenter.ms	ok	**IP:** 13.107.246.70 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
appgallery.huawei.com	ok	**IP:** 80.158.49.80 **Country:** Germany **Region:** Schleswig-Holstein **City:** Kiel **Latitude:** 54.321331 **Longitude:** 10.134890 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
mobile.events.data.microsoft.com	ok	**IP:** 40.79.173.41 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map
search.brave.com	ok	**IP:** 3.175.64.2 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
translations.telegram.org	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
maps.googleapis	ok	No Geolocation information available.
player.vimeo.com	ok	**IP:** 162.159.138.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
suggestqueries.google.com	ok	**IP:** 142.250.69.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
core.telegram.org	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
promote.telegram.org	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
legal.yahoo.com	ok	**IP:** 98.137.11.157 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
aomediacodec.github.io	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
api.bing.com	ok	**IP:** 13.107.5.80 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
privacy.microsoft.com	ok	**IP:** 23.217.131.226 **Country:** Russian Federation **Region:** Chelyabinskaya oblast' **City:** Chelyabinsk **Latitude:** 55.154442 **Longitude:** 61.429722 **View:** Google Map
maps.google.com	ok	**IP:** 142.250.73.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
telegram.org	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
stripe.com	ok	**IP:** 52.10.212.243 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
tgb-playground.smart-glocal.com	ok	**IP:** 99.83.179.90 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
messenger.telegram.org	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

DOMAIN	STATUS	GEOLOCATION
www.youtube.com	ok	**IP:** 142.250.217.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 142.250.73.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
tgb.smart-glocal.com	ok	**IP:** 75.2.95.23 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
ss3.4sqi.net	ok	**IP:** 151.101.22.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
web.telegram.org	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
twitter.com	ok	**IP:** 162.159.140.229 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
search.yahoo.com	ok	**IP:** 98.136.144.138 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map
api.stripe.com	ok	**IP:** 54.68.165.206 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
coub.com	ok	**IP:** 95.213.253.85 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
api.appcenter.ms	ok	**IP:** 13.107.246.70 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
tonviewer.com	ok	**IP:** 104.26.6.189 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
tmessages2.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
usher.ttvnw.net	ok	**IP:** 18.64.67.26 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.tensorflow.org	ok	**IP:** 142.251.34.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dns.google.com	ok	**IP:** 8.8.4.4 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
youtube.com	ok	**IP:** 142.250.217.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
attheme.org	ok	No Geolocation information available.
policies.google.com	ok	**IP:** 142.251.34.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 142.250.73.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
in.appcenter.ms	ok	**IP:** 52.247.72.241 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.webrtc.org	ok	**IP:** 142.251.34.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sugg.search.yahoo.net	ok	**IP:** 98.136.144.138 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map
www.aparat.com	ok	**IP:** 185.147.178.13 **Country:** Iran (Islamic Republic of) **Region:** Tehran **City:** Tehran **Latitude:** 35.694389 **Longitude:** 51.421509 **View:** Google Map

EMAILS

EMAIL	FILE
sms@telegram.org	org/telegram/ui/PassportActivity.java
login@stel.com recover@telegram.org sms@telegram.org	org/telegram/ui/LoginActivity.java

EMAIL	FILE
support@stripe.com	com/stripe/android/net/StripeApiHandler.java
reports@stel.com□□ reports@stel.com sms@telegram.org	Android String Resource
android-sdk-releaser@oouc14.prod	lib/x86/liblanguage_id_l2c_jni.so
android-sdk-releaser@oouc14.prod	lib/armeabi-v7a/liblanguage_id_l2c_jni.so
android-sdk-releaser@oouc14.prod	lib/arm64-v8a/liblanguage_id_l2c_jni.so
appro@openssl.org	lib/arm64-v8a/libtmessages.49.so
android-sdk-releaser@oouc14.prod	lib/x86_64/liblanguage_id_l2c_jni.so
appro@openssl.org	lib/x86_64/libtmessages.49.so
android-sdk-releaser@oouc14.prod	apktool_out/lib/x86/liblanguage_id_l2c_jni.so
android-sdk-releaser@oouc14.prod	apktool_out/lib/armeabi-v7a/liblanguage_id_l2c_jni.so
android-sdk-releaser@oouc14.prod	apktool_out/lib/arm64-v8a/liblanguage_id_l2c_jni.so
appro@openssl.org	apktool_out/lib/arm64-v8a/libtmessages.49.so
android-sdk-releaser@oouc14.prod	apktool_out/lib/x86_64/liblanguage_id_l2c_jni.so
appro@openssl.org	apktool_out/lib/x86_64/libtmessages.49.so

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Microsoft Visual Studio App Center Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/243
Microsoft Visual Studio App Center Crashes	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/238

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"YourPassword" : "□□□□"
"NotificationsPrivateChats" : "Privéchats"
"UseProxySecret" : "Segredo"
"LoginPassword" : "Пароль"
"UseProxyUsername" : "Gebruiker"
"UseProxyUsername" : "Username"
"UseProxyPassword" : "Password"
"UseProxyUsername" : "Usuario"
"NotificationHiddenChatUserName" : "User"
"UseProxySecret" : "Segreto "
"com.google.firebase.crashlytics.mapping_file_id" : "baee002a0fa9427aac70a5825255531e"

POSSIBLE SECRETS
"LoginPassword" : "Wachtwoord"
"Username" : "Gebruikersnaam"
"UseProxyPassword" : "Senha"
"UseProxySecret" : "Secret"
"UseProxyPassword" : "Passwort"
"NotificationHiddenChatUserName" : "مستخدم"
"LoginPassword" : "Contraseña"
"ReplyToUser" : "□□"
"LoginPassword" : "Senha"
"LoginPassword" : "□□□□"
"NotificationHiddenChatUserName" : "□□□"
"UseProxySecret" : "السر"
"UseProxySecret" : "Sleutel"
"BotStarsButtonWithdrawShortUntil" : "Withdraw"
"UseProxyUsername" : "Benutzername"
"UseProxyUsername" : "□□□□"
"LoginPassword" : "Passwort"

POSSIBLE SECRETS
"NotificationHiddenChatUserName" : "Nutzer"
"UseProxyPassword" : "Contraseña"
"google_crash_reporting_api_key" : "AIzaSyA-t0jLPjUt2FxrA8VPK2EiYHcYcboIR6k"
"ReplyToUser" : "Rispondi"
"NotificationHiddenChatUserName" : "Gebruiker"
"NotificationHiddenChatUserName" : "Usuario"
"Username" : "Username"
"ReplyToUser" : "Responder"
"TypePrivate" : "Private"
"YourPassword" : "Пароль"
"ReplyToUser" : "رد"
"NotificationHiddenChatUserName" : "Utente"
"ReplyToUser" : "Reageren"
"ProfileActionsEditUsername" : "Username"
"AutodownloadPrivateChats" : "Chats"
"LoginPassword" : "Password"
"ReplyToUser" : "Antworten"

POSSIBLE SECRETS
"google_api_key" : "AIzaSyA-t0jLPjUt2FxrA8VPK2EiYHcYcboIR6k"
"TypePrivateGroup" : "Private"
"NotificationsPrivateChats" : "Einzelchats"
"UseProxyPassword" : "□□□□"
"UseProxySecret" : "Clave"
"UseProxyPassword" : "Wachtwoord"
"firebase_database_url" : "https://tmessages2.firebaseio.com"
"AutodownloadPrivateChats" : "Einzelchats"
"NotificationHiddenChatUserName" : "Usuário"
"UseProxySecret" : "Schlüssel"
014b35b6184100b085b0d0572f9b5103
9a04f079-9840-4286-ab92-e65be0885f95
ABVGDE2JZIQKLMNOPRSTUFHC34WXY9678
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
e2719d58-a985-b3c9-781a-b030af78d30e
123456789101112365489756653622 3
f9726602-67c9-48d2-b5d0-4761f1c1a8f3

POSSIBLE SECRETS
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
BoostingGiveawayHowItWorksSubTextSeveralEnd1
BoostingGiveawayHowItWorksSubTextDateSeveralEnd1
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
470fa2b4ae81cd56ecbcda9735803434cec591fa

SCAN LOGS

Timestamp	Event	Error
2025-11-08 20:20:48	Generating Hashes	OK
2025-11-08 20:20:49	Extracting APK	OK
2025-11-08 20:20:49	Unzipping	OK
2025-11-08 20:20:52	Parsing APK with androguard	OK
2025-11-08 20:20:53	Extracting APK features using aapt/aapt2	OK

2025-11-08 20:20:54	Getting Hardcoded Certificates/Keystores	OK
2025-11-08 20:21:03	Parsing AndroidManifest.xml	OK
2025-11-08 20:21:03	Extracting Manifest Data	OK
2025-11-08 20:21:03	Manifest Analysis Started	OK
2025-11-08 20:21:04	Performing Static Analysis on: Telegram Beta (org.telegram.messenger.beta)	OK
2025-11-08 20:21:05	Fetching Details from Play Store: org.telegram.messenger.beta	OK
2025-11-08 20:21:05	Checking for Malware Permissions	OK
2025-11-08 20:21:05	Fetching icon path	OK
2025-11-08 20:21:05	Library Binary Analysis Started	OK
2025-11-08 20:21:05	Analyzing lib/x86/liblanguage_id_l2c_jni.so	OK
2025-11-08 20:21:05	Analyzing lib/x86/libtmessages.49.so	OK
2025-11-08 20:21:06	Analyzing lib/armeabi-v7a/liblanguage_id_l2c_jni.so	OK

2025-11-08 20:21:06	Analyzing lib/armeabi-v7a/libtmessages.49.so	OK
2025-11-08 20:21:07	Analyzing lib/arm64-v8a/liblanguage_id_l2c_jni.so	OK
2025-11-08 20:21:07	Analyzing lib/arm64-v8a/libtmessages.49.so	OK
2025-11-08 20:21:08	Analyzing lib/x86_64/liblanguage_id_l2c_jni.so	OK
2025-11-08 20:21:08	Analyzing lib/x86_64/libtmessages.49.so	OK
2025-11-08 20:21:09	Analyzing apktool_out/lib/x86/liblanguage_id_l2c_jni.so	OK
2025-11-08 20:21:09	Analyzing apktool_out/lib/x86/libtmessages.49.so	OK
2025-11-08 20:21:10	Analyzing apktool_out/lib/armeabi-v7a/liblanguage_id_l2c_jni.so	OK
2025-11-08 20:21:10	Analyzing apktool_out/lib/armeabi-v7a/libtmessages.49.so	OK
2025-11-08 20:21:11	Analyzing apktool_out/lib/arm64-v8a/liblanguage_id_l2c_jni.so	OK
2025-11-08 20:21:11	Analyzing apktool_out/lib/arm64-v8a/libtmessages.49.so	OK
2025-11-08 20:21:12	Analyzing apktool_out/lib/x86_64/liblanguage_id_l2c_jni.so	OK

2025-11-08 20:21:12	Analyzing apktool_out/lib/x86_64/libtmessages.49.so	OK
2025-11-08 20:21:13	Reading Code Signing Certificate	OK
2025-11-08 20:21:16	Running APKiD 3.0.0	OK
2025-11-08 20:21:29	Detecting Trackers	OK
2025-11-08 20:21:37	Decompiling APK to Java with JADX	OK
2025-11-08 20:23:04	Converting DEX to Smali	OK
2025-11-08 20:23:04	Code Analysis Started on - java_source	OK
2025-11-08 20:23:16	Android SBOM Analysis Completed	OK
2025-11-08 20:24:28	Android SAST Completed	OK
2025-11-08 20:24:28	Android API Analysis Started	OK
2025-11-08 20:25:31	Android API Analysis Completed	OK
2025-11-08 20:25:32	Android Permission Mapping Started	OK

2025-11-08 20:27:45	Android Permission Mapping Completed	OK
2025-11-08 20:27:46	Android Behaviour Analysis Started	OK
2025-11-08 20:29:53	Android Behaviour Analysis Completed	OK
2025-11-08 20:29:53	Extracting Emails and URLs from Source Code	OK
2025-11-08 20:30:10	Email and URL Extraction Completed	OK
2025-11-08 20:30:10	Extracting String data from APK	OK
2025-11-08 20:30:11	Extracting String data from SO	OK
2025-11-08 20:30:13	Extracting String data from Code	OK
2025-11-08 20:30:13	Extracting String values and entropies from Code	OK
2025-11-08 20:30:22	Performing Malware check on extracted domains	OK
2025-11-08 20:30:32	Saving to Database	OK

performing static and dynamic analysis.