APK Static Analysis Report

SSL/TLS Misconfigurations

Method: setSSLSocketFactory
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: getDefaultSSLSocketFactory
Class: Ljavax/net/ssl/HttpsURLConnection;
Description: Potential SSL/TLS misuse detected

Method: <init>
Class: Ljavax/net/ssl/SSLSocketFactory;
Description: Potential SSL/TLS misuse detected

Method: createSocket
Class: Ljavax/net/ssl/SSLSocketFactory;
Description: Potential SSL/TLS misuse detected

Method: getDefaultCipherSuites
Class: Ljavax/net/ssl/SSLSocketFactory;
Description: Potential SSL/TLS misuse detected

Method: getSupportedCipherSuites
Class: Ljavax/net/ssl/SSLSocketFactory;
Description: Potential SSL/TLS misuse detected

Method: getDefault
Class: Ljavax/net/ssl/SSLContext;
Description: Potential SSL/TLS misuse detected

Method: getSupportedSSLParameters
Class: Ljavax/net/ssl/SSLContext;
Description: Potential SSL/TLS misuse detected

Method: getProtocols
Class: Ljavax/net/ssl/SSLParameters;
Description: Potential SSL/TLS misuse detected

Method: getEnabledProtocols
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: setEnabledProtocols
Class: Ljavax/net/ssl/SSLSocket;
Description: Potential SSL/TLS misuse detected

Method: getInstance
Class: Ljava/security/cert/CertificateFactory;
Description: Potential SSL/TLS misuse detected

Method: generateCertificate
Class: Ljava/security/cert/CertificateFactory;
Description: Potential SSL/TLS misuse detected

Method: getEncoded
Class: Ljava/security/cert/Certificate;
Description: Potential SSL/TLS misuse detected

Cryptographic Misuse

Method: getCertificateSHA1Fingerprint
Class: Lorg/telegram/messenger/AndroidUtilities;
Description: Use of weak cryptographic algorithm: SHA1

Method: MD5
Class: Lorg/telegram/messenger/Utilities;
Description: Use of weak cryptographic algorithm: MD5

Method: computeSHA1
Class: Lorg/telegram/messenger/Utilities;
Description: Use of weak cryptographic algorithm: SHA1

Method: computeSHA1
Class: Lorg/telegram/messenger/Utilities;
Description: Use of weak cryptographic algorithm: SHA1

Method: computeSHA1
Class: Lorg/telegram/messenger/Utilities;
Description: Use of weak cryptographic algorithm: SHA1

Method: computeSHA1
Class: Lorg/telegram/messenger/Utilities;
Description: Use of weak cryptographic algorithm: SHA1

Method: $r8$lambda$OvFE7x-vB7HKZttVO-pHveMD5vw
Class: Lorg/telegram/ui/Stories/StoriesController$StoriesList;
Description: Use of weak cryptographic algorithm: MD5

Method: $r8$lambda$2fhSTKtcO2Wf9EJwDESjDHhYp7o
Class: Lorg/telegram/ui/Stories/recorder/StoryRecorder;
Description: Use of weak cryptographic algorithm: DES

Method: $r8$lambda$-kxpx6OayDES4Uhf2uTnVyDLic0
Class: Lorg/telegram/ui/Stories/recorder/EmojiBottomSheet;
Description: Use of weak cryptographic algorithm: DES

Method: $r8$lambda$vmJ5kIAKrgDESDBY9mSNmDfVqRs
Class: Lorg/telegram/messenger/voip/VoIPService;
Description: Use of weak cryptographic algorithm: DES

Method: $r8$lambda$cEg1-Gl7DESnlWogY9ho4fymeTY
Class: Lorg/telegram/ui/LoginActivity$LoginActivitySmsView;
Description: Use of weak cryptographic algorithm: DES

Method: $r8$lambda$35EsBeU5mY_6hz6rMvZSDESGjqI
Class: Lorg/telegram/ui/PasscodeActivity;
Description: Use of weak cryptographic algorithm: DES

Access Control Issues

Component: org.telegram.messenger.GoogleVoiceClientActivity
Type: activity
Description: Activity exported without proper access control

Component: org.telegram.ui.LaunchActivity
Type: activity
Description: Activity exported without proper access control

Component: org.telegram.ui.ShareActivity
Type: activity
Description: Activity exported without proper access control

Component: org.telegram.ui.ExternalActionActivity
Type: activity
Description: Activity exported without proper access control

Component: org.telegram.ui.ChatsWidgetConfigActivity
Type: activity
Description: Activity exported without proper access control

Component: org.telegram.ui.ContactsWidgetConfigActivity
Type: activity
Description: Activity exported without proper access control

Component: org.telegram.messenger.OpenChatReceiver
Type: activity
Description: Activity exported without proper access control

Component: org.telegram.messenger.OpenAttachedMenuBotReceiver
Type: activity
Description: Activity exported without proper access control

Component: org.telegram.messenger.GcmPushListenerService
Type: service
Description: Service exported without proper access control

Component: org.telegram.messenger.GoogleVoiceClientService
Type: service
Description: Service exported without proper access control

Component: org.telegram.messenger.AuthenticatorService
Type: service
Description: Service exported without proper access control

Component: org.telegram.messenger.ContactsSyncAdapterService
Type: service
Description: Service exported without proper access control

Component: org.telegram.messenger.BringAppForegroundService
Type: service
Description: Service exported without proper access control

Component: org.telegram.messenger.NotificationsService
Type: service
Description: Service exported without proper access control

Component: org.telegram.messenger.VideoEncodingService

Type: service
Description: Service exported without proper access control

Component: org.telegram.ui.Stories.recorder.StoryUploadingService
Type: service
Description: Service exported without proper access control

Component: org.telegram.messenger.ImportingService
Type: service
Description: Service exported without proper access control

Component: org.telegram.messenger.LocationSharingService
Type: service
Description: Service exported without proper access control

Component: org.telegram.messenger.MusicPlayerService
Type: service
Description: Service exported without proper access control

Component: org.telegram.messenger.MusicBrowserService
Type: service
Description: Service exported without proper access control

Component: org.telegram.messenger.voip.TelegramConnectionService
Type: service
Description: Service exported without proper access control

Component: com.google.android.gms.auth.api.signin.RevocationBoundService
Type: service
Description: Service exported without proper access control

Component: androidx.sharetarget.ChooserTargetServiceCompat
Type: service
Description: Service exported without proper access control

Component: org.telegram.messenger.SmsReceiver
Type: receiver
Description: Receiver exported without proper access control

Component: org.telegram.messenger.RefererReceiver
Type: receiver
Description: Receiver exported without proper access control

Component: com.google.firebase.iid.FirebaseInstanceIdReceiver
Type: receiver
Description: Receiver exported without proper access control

Component: org.telegram.messenger.voip.CallNotificationSoundProvider
Type: provider
Description: Provider exported without proper access control