MOBSF

ANDROID STATIC ANALYSIS REPORT

DHL (1.0)

File Name:	DHL.apk
Package Name:	com.tencent.mm
Average CVSS Score:	7.5
App Security Score:	100/100 (LOW RISK)
Scan Date:	Jan. 28, 2021, 11:54 p.m.

FILE INFORMATION

File Name: DHL.apk
Size: 3.86MB
MD5: ef330033827e283c19b54077f544aa54
SHA1: 8db6fdfe3fdcf96aeae2f515f3230912a7195ad5
SHA256: 37d03d4063c3142aa5bfeb0daf92f95f05b605aedf293017181e57bd1bf1df65

APP INFORMATION

App Name: DHL
Package Name: com.tencent.mm
Main Activity: com.tencent.mm.MainActivity
Target SDK: 28
Min SDK: 23
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 7
Services: 4
Receivers: 3
Providers: 0
Exported Activities: 2
Exported Services: 3
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2008-02-29 01:33:46+00:00
Valid To: 2035-07-17 01:33:46+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
Serial Number: 0x936eacbe07f201df
Hash Algorithm: sha1
md5: e89b158e4bcf988ebd09eb83f5378e87
sha1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
sha256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
sha512: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75

STATUS	DESCRIPTION
secure	Application is signed with a code signing certificate
warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android <7.0
warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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_SMS	dangerous	edit SMS or MMS	Allows application to write to SMS messages stored on your phone or SIM card. Malicious applications may delete your messages.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.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.QUERY_ALL_PACKAGES	normal		Allows query of any normal app on the device, regardless of manifest declarations.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal		Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.REQUEST_DELETE_PACKAGES	normal		Allows an application to request deleting packages.

APKID ANALYSIS

FILE	DETAILS

classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dexlib 2.x</td></tr><tr><td>Obfuscator</td><td>unreadable field names unreadable method names</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.tencent.mm.ComposeSmsActivity	Schemes: sms://, smsto://, mms://, mmsto://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Application Data can be Backed up [android:allowBackup=true]	medium	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Service (com.tencent.mm.MyNotificationListener) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_SERVICE [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. 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.
4	Service (com.tencent.mm.ForegroundService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity (com.tencent.mm.ComposeSmsActivity) is not Protected. An intent-filter exists.	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.
	Broadcast Receiver (com.tencent.mm.SmsReceiver) is Protected by a permission, but the protection level of the		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

6	permission should be checked. Permission: android.permission.BROADCAST_SMS [android:exported=true]	high	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.
7	Broadcast Receiver (com.tencent.mm.MmsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BROADCAST_WAP_PUSH [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	Broadcast Receiver (com.tencent.mm.BootReceiver) is not Protected. An intent-filter exists.	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
9	Service (com.tencent.mm.HeadlessSmsSendService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.SEND_RESPOND_VIA_MESSAGE [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. 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.
10	Activity (com.tencent.mm.IntentStarter) is not Protected. An intent-filter exists.	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 (high) CWE: CWE-532 Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/whatsapp/conversation/conversationrow/album/MediaAlbumActivity.java com/whatsapp/conversation/ConversationVideoPictureInPictureActivity.java bitter/jnibridge/JNIBridge.java com/whatsapp/components/TextAndDateLayout.java X/AnonymousClass00b.java org/fmod/a.java com/whatsapp/bloks/ui/BloksDialogFragment.java com/whatsapp/videoplayback/VideoSurfaceView.java com/whatsapp/conversation/ConversationListView.java com/whatsapp/conversation/conversationrow/message/StarredMessagesActivity.java org/fmod/FMODAudioDevice.java com/whatsapp/conversation/conversationrow/ConversationPaymentRowTransactionLayout.java com/whatsapp/biz/product/view/activity/ProductDetailActivity.java com/unity3d/player/p.java com/whatsapp/components/PhoneNumberEntry.java com/whatsapp/biz/catalog/CatalogMediaCard.java com/unity3d/player/g.java
2	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	CVSS V2: 0 (info) OWASP MASVS: MSTG-STORAGE-10	com/unity3d/player/UnityPlayer.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
2	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to ['address book'].
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
6	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files in non-volatile memory.
7	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
8	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
9	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
wa.me	good	**IP:** 69.171.250.60 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.88969 **View:** Google Map

URLS

URL	FILE
https://wa.me	com/whatsapp/biz/catalog/ShareCatalogLinkActivity.java
https://wa.me	com/whatsapp/biz/catalog/ShareProductLinkActivity.java

PLAYSTORE INFORMATION

Title: WeChat

Score: 3.6172044 **Installs:** 100,000,000+ **Price:** 0 **Android Version Support:** 5.0 and up **Category:** Communication **Play Store URL:** com.tencent.mm

Developer Details: WeChat, WeChat, 2747 Park Blvd., Palo Alto, California, USA, 94306, http://www.wechat.com, support@wechat.com,

Release Date: Jan 30, 2011 **Privacy Policy:** Privacy link

Description:

WeChat is more than a messaging and social media app – it is a lifestyle for over one billion users across the world. Chat and make calls with friends, read news and use local services in Official Accounts and Mini Programs, play fun games with friends, enjoy mobile payment features with WeChat Pay, and much more. Why do over one billion people use WeChat? Well... - MORE WAYS TO CHAT: Message friends using text, photo, voice, video, location sharing, and more. Create group chats with up to 500 members. - VOICE & VIDEO CALL: High-quality voice and video calls to anywhere in the world. Make group video calls with up to 9 people. - REAL-TIME LOCATION: Not good at explaining directions? Share your real-time location with the press of a button. - MOMENTS: Share your favorite moments. Post photos, videos, and more to your Moments stream. - TIME CAPSULE (NEW!): Share glimpses of your day. Record short videos to post in your Time Capsule before they disappear in 24 hours. - STICKER GALLERY: Browse thousands of fun, animated stickers to help express yourself in chats, including stickers with your favorite cartoon and movie characters. - CUSTOM STICKERS: Make chatting more unique with custom stickers and the new Selfie Stickers feature. - OFFICIAL ACCOUNTS: Tons of accounts to follow with original content and news for your reading pleasure. - MINI PROGRAMS: Countless third-party services all within the WeChat app that don't require additional installation, saving you precious phone storage and time. - TOP STORIES: See the latest articles your friends are reading and discover all kinds of interesting content. - GAMES: Have fun and compete with friends in a huge selection of WeChat Mini Games and Tencent Games (*only available in certain regions). - WECHAT PAY: Enjoy the convenience of world-leading mobile payment features with WeChat Pay and Wallet (*only available in certain regions). - WECHAT OUT: Make calls to mobile phones and landlines around the globe at super low rates (*only available in certain regions). - LANGUAGE SUPPORT: Localized in 20 different languages and can translate friends' messages and Moments posts. - BETTER PRIVACY: Giving you the highest level of control over your privacy, WeChat is the only messaging app to be certified by TRUSTe. - AND MUCH MORE: Exercise with friends on WeRun, scan QR codes, and much more.

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.3.0 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.