

M

McDonald's Denmark (3.1.3)

File Name:	McDonald's Danmark_3.1.3_Apkpure.apk
Package Name:	com.apegroup.mcdonaldsdenmark
Scan Date:	May 3, 2023, 12:32 p.m.
App Security Score:	37/100 (HIGH RISK)
Grade:	C
Trackers Detection:	7/428

FINDINGS SEVERITY

ॠ HIGH	▲ MEDIUM	i INFO	✓ SECURE	◎ HOTSPOT
2	6	1	0	1

FILE INFORMATION

File Name: McDonald's Danmark_3.1.3_Apkpure.apk

Size: 16.9MB

MD5: c76eb582d2d56d4be17ea929103e43a8

SHA1: 9c6cd61a48afd792074fabb1a3ae3d3f8a929200

SHA256: 45916dc47b3daa1abed7dfd1950ac3e8e7350f22b7fad87c424525acdef685a9

i APP INFORMATION

App Name: McDonald's Denmark

Package Name: com.apegroup.mcdonaldsdenmark **Main Activity:** mcdonalds.basic.McdonaldsHomeActivity

Target SDK: 21 Min SDK: 15 Max SDK:

Android Version Name: 3.1.3

APP COMPONENTS

Activities: 18 Services: 20 Receivers: 2 Providers: 2

Exported Activities: 0 Exported Services: 0 Exported Receivers: 2 Exported Providers: 1



APK is signed v1 signature: True v2 signature: True v3 signature: False

Found 1 unique certificates

Subject: C=DK

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2012-08-23 08:16:25+00:00 Valid To: 2062-08-11 08:16:25+00:00

Issuer: C=DK

Serial Number: 0x5035e6d9 Hash Algorithm: sha1

md5: 8856d4468408e5549f17d47a649921eb

sha1: 1ac669cfb188bf74aa47692939cb8604ac9927f7

sha256: 65101cc1f3a4a20fa5df01bb13b84cc4c904da5c01645547b0281fdfa2e1ebe5

sha512: ef820e60b0e4a3eb7dac0a083c494a4a305bed14045f020e4a0faed51e7ae2bc9ab63a257195cabc791b98e88b35cda9f9bef5e602d5245b70f11bfa76071ac4

PublicKey Algorithm: rsa

Bit Size: 1024

Fingerprint: 50134d4ccd3b1253a7d78de913a7215b6b366dc924e101bce0f1d51a984d75ce

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.apegroup.mcdonaldsdenmark.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.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_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.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.RUN_INSTRUMENTATION	unknown	Unknown permission	Unknown permission from android reference

M APKID ANALYSIS

FILE	DETAILS		
	FINDINGS	DETAILS	
classes.dex	Anti-VM Code	Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check network operator name check	
	Compiler	dx	

FILE	DETAILS		
classes2.dex	FINDINGS	DETAILS	
Classesz.ucx	Compiler	dx	

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
mcdonalds.basic.McdonaldsHomeActivity	Schemes: mcd://, @string/urlScheme://, Hosts: @string/urlHost, Path Prefixes: @string/urlPathPrefix,

△ NETWORK SECURITY

N	10	SCOPE	SEVERITY	DESCRIPTION
---	----	-------	----------	-------------

CERTIFICATE ANALYSIS

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

Q MANIFEST ANALYSIS

HIGH: 0 | WARNING: 4 | INFO: 0 | SUPPRESSED: 0

N	10	ISSUE	SEVERITY	DESCRIPTION
1		App can be installed on a vulnerable Android version [minSdk=15]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 to receive reasonable security updates.
2		Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Broadcast Receiver (mcdonalds.core.lib.service.gcm.GCMBroadcastReceiver) 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.
4	Content Provider (mcdonalds.restaurants.search.RestaurantsSuggestionProvider) would not be Protected if the application ran on a device where the the API level was less than 17. [Content Provider, targetSdkVersion >= 17]	warning	The Content Provider(Content Provider) would be exported if the application ran on a device where the the API level was less than 17. In that situation, it would be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1 | SECURE: 0 | SUPPRESSED: 0

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	com/adform/adformtrackingsdk/utils/Netw orkUtils.java com/dm/zbar/android/scanner/CameraPrev iew.java



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/mips/liblept.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector- all to enable stack canaries.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.
2	lib/mips/libtess.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector- all to enable stack canaries.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/armeabi-v7a/liblept.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.
4	lib/armeabi-v7a/libiconv.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/armeabi-v7a/libzbarjni.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.
6	lib/armeabi-v7a/libtess.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/armeabi/liblept.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.
8	lib/armeabi/libiconv.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	lib/armeabi/libzbarjni.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.
10	lib/armeabi/libtess.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	lib/x86/liblept.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.
12	lib/x86/libiconv.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	lib/x86/libzbarjni.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.
14	lib/x86/libtess.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application use no DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity', 'location', 'camera'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FCS_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.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	IP: 104.18.23.19 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
track.adform.net	ok	IP: 37.157.5.133 Country: Denmark Region: Hovedstaden City: Copenhagen Latitude: 55.675941 Longitude: 12.565530 View: Google Map



EMAIL	FILE
6h@fo.lwft w9oi_2nhels4u@dlilycclglhl.5jlcg_bqh yay@y.u5vcghyy	lib/armeabi-v7a/libiconv.so
6h@fo.lwft w9oi_2nhels4u@dlilycclglhl.5jlcg_bqh yay@y.u5vcghyy	lib/armeabi/libiconv.so
yay@y.u5vcghyy 6h@fo.lwft w9oi_2nhels4u@dlilycclglhl.5jlcg_bqh	lib/x86/libiconv.so

** TRACKERS

TRACKER	CATEGORIES	URL
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
HockeyApp	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/26

TRACKER	CATEGORIES	URL

HARDCODED SECRETS

Report Generated by - MobSF v3.6.6 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.

© 2023 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.