MOBSF

ANDROID STATIC ANALYSIS REPORT

foodpanda (24.13.0)

File Name:	foodpanda.apk
Package Name:	com.global.foodpanda.android
Scan Date:	Aug. 26, 2024, 8:37 p.m.
App Security Score:	48/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	6/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	25	3	2	1

FILE INFORMATION

File Name: foodpanda.apk
Size: 29.1MB
MD5: ef6247638bd6c797655233ff4fa7aba7
SHA1: 6651e666d7b65dd1c767823340a3b1cac8f2b34f
SHA256: d4b12cfda0d4c114ad4f9109fc7b0431bab8b0d5aa6c409de2c86c592949c06b

APP INFORMATION

App Name: foodpanda
Package Name: com.global.foodpanda.android
Main Activity:
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 24.13.0

Android Version Code: 241300184

APP COMPONENTS

Activities: 184
Services: 16
Receivers: 21
Providers: 10
Exported Activities: 8
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=PT, ST=Porto, L=Porto, O=Rocket Internet, OU=SilverOak, CN=Ricardo Dourado
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-11-15 11:34:37+00:00
Valid To: 2040-04-02 11:34:37+00:00
Issuer: C=PT, ST=Porto, L=Porto, O=Rocket Internet, OU=SilverOak, CN=Ricardo Dourado
Serial Number: 0x7941263b
Hash Algorithm: sha256
md5: 6114ede7e27daff0311f8748ec18185d
sha1: a5b05d45938e7795f0df9a81924a32d32c0abe63
sha256: af472590adc7f390d8aa24bdb2b049591efdf35b0a0837582890aa7d2276c663
sha512: 43f2b3de38cb0006e14fb8f649a6c6415bc7322b4245dca01ae3c2392da023ec7798127be1341e1951303b838bbac153052b46e0a05f5bb92de7fcd7d5477cb0
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 04fe0c011b70310159b0e4547d25c4cab59f5b92d7da6d0eae99edb977a0f220
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.adjust.preinstall.READ_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.global.foodpanda.android.permission.A4S_SEND	unknown	Unknown permission	Unknown permission from android reference
.permission.MAPS_RECEIVE	unknown	Unknown permission	Unknown permission from android reference
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.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.READ_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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.HIGH_SAMPLING_RATE_SENSORS	normal	Access higher sampling rate sensor data	Allows an app to access sensor data with a sampling rate greater than 200 Hz.

PERMISSION	STATUS	INFO	DESCRIPTION
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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
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.
com.global.foodpanda.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<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</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>Anti-VM Code</td><td>Build.MANUFACTURER check
Build.BRAND check
Build.DEVICE check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes6.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.BOARD check
Build.TAGS check
network operator name check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
<tr><td>classes7.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
de.foodora.android.ui.launcher.LauncherActivity	Schemes: hungry://, foodpanda://, https://, Hosts: foodpanda.com, www.foodpanda.pk, www.foodpanda.sg, www.foodpanda.my, www.foodpanda.com.bd, www.foodpanda.co.th, www.foodpanda.hk, www.foodpanda.com.tw, www.foodpanda.ph, www.foodpanda.com.kh, www.foodpanda.la, www.foodpanda.com.mm, www.foodpanda.bg, www.foodpanda.ro, www.foodpanda.co.jp, Paths: /, /corporate, Path Prefixes: /chain, /city, /cuisine, /darkstore, /groceries, /login, /item, /restaurant, /restaurants, /shop, /special-menus, /payments, /pandapay, /yuu, Path Patterns: /..*/,
com.deliveryhero.auth.oauth.OauthActivity	Schemes: foodpanda-openid://, Hosts: auth, Path Patterns: /callback, /callback/.*,
com.deliveryhero.auth.ui.klarna.KlarnaLoginActivity	Schemes: foodpanda-klarna://, Hosts: @string/klarna_return_host,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.global.foodpanda.android,
com.deliveryhero.payment.cashier.PaymentActivity	Schemes: foodpanda-cashier://, Hosts: *, Path Patterns: /cashier-payment,
com.deliveryhero.cobrandedcard.applink.ui.CobrandedCardDeepLinkActivity	Schemes: foodpanda-cobrandedcard://,
com.deliveryhero.inapprating.InAppRatingActivity	Schemes: foodpanda-iar://,

NETWORK SECURITY

HIGH: 0 | WARNING: 0 | INFO: 0 | SECURE: 0

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | 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.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 13 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 6.0-6.0.1, [minSdk=23]	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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Activity-Alias (de.foodora.android.ui.launcher.LauncherActivity) 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.
4	Activity (com.deliveryhero.auth.oauth.OauthActivity) 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.
5	Activity (com.deliveryhero.auth.ui.klarna.KlarnaLoginActivity) 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.
6	Activity (com.facebook.CustomTabActivity) 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.deliveryhero.payment.wallet.wechat.WeChatEntryActivity) 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	Activity (com.deliveryhero.payment.cashier.PaymentActivity) 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
9	Activity (com.deliveryhero.cobrandedcard.applink.ui.CobrandedCardDeepLinkActivity) 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.
10	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.
11	Activity (com.deliveryhero.inapprating.InAppRatingActivity) 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.
12	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
13	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
14	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
15	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: 10 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	bo/app/d1.java com/adjust/sdk/Util.java defpackage/bmz.java defpackage/dw80.java defpackage/fm90.java defpackage/g0a0.java defpackage/i5a.java defpackage/ie80.java defpackage/jlr.java defpackage/k2.java defpackage/m330.java defpackage/nr30.java defpackage/o6s.java defpackage/qka0.java defpackage/tio.java defpackage/uau.java defpackage/uud.java defpackage/v4v.java defpackage/vd90.java defpackage/w4v.java defpackage/wou.java defpackage/xlt.java defpackage/xx80.java defpackage/ypv.java defpackage/yti.java j$/util/concurrent/ThreadLocalRandom.java
				com/adjust/sdk/Logger.java com/adjust/sdk/oaid/AdjustOaid.java com/adjust/sdk/oaid/Util.java com/adjust/sdk/sig/NativeLibHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/adjust/sdk/sig/SignerInstance.java com/bumptech/glide/a.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/manager/b.java com/deliveryhero/app/App.java com/deliveryhero/chatui/view/chatroom/ChatFragment.java com/deliveryhero/performance/core/AppStartupTracesInitializer.java com/deliveryhero/performance/core/compose/LifecycleObserver.java com/hbb20/CountryCodePicker.java com/hbb20/a.java com/klarna/mobile/sdk/core/log/LogExtensionsKt.java com/klarna/mobile/sdk/core/log/Logger.java com/makeramen/roundedimageview/RoundedImageView.java com/shakebugs/shake/Shake.java com/shakebugs/shake/internal/a4.java com/shakebugs/shake/internal/b1.java com/shakebugs/shake/internal/c1.java com/shakebugs/shake/internal/f.java com/shakebugs/shake/internal/utils/m.java com/tencent/mm/opensdk/channel/MMessageActV2.java com/tencent/mm/opensdk/channel/a/a.java com/tencent/mm/opensdk/diffdev/DiffDevOAuthFactory.java com/tencent/mm/opensdk/diffdev/a/a.java com/tencent/mm/opensdk/diffdev/a/b.java com/tencent/mm/opensdk/diffdev/a/c.java com/tencent/mm/opensdk/modelbiz/ChooseCardFromWXCardPackage.java com/tencent/mm/opensdk/modelbiz/Subscrib

NO	ISSUE	SEVERITY	STANDARDS	FILES
				eMessage.java com/tencent/mm/opensdk/modelbiz/SubscribeMiniProgramMsg.java com/tencent/mm/opensdk/modelbiz/WXChannelBaseJumpInfo.java com/tencent/mm/opensdk/modelbiz/WXChannelJumpMiniProgramInfo.java com/tencent/mm/opensdk/modelbiz/WXChannelJumpUrlInfo.java com/tencent/mm/opensdk/modelbiz/WXChannelOpenFeed.java com/tencent/mm/opensdk/modelbiz/WXChannelOpenLive.java com/tencent/mm/opensdk/modelbiz/WXChannelOpenProfile.java com/tencent/mm/opensdk/modelbiz/WXChannelShareVideo.java com/tencent/mm/opensdk/modelbiz/WXInvoiceAuthInsert.java com/tencent/mm/opensdk/modelbiz/WXLaunchMiniProgram.java com/tencent/mm/opensdk/modelbiz/WXLaunchMiniProgramWithToken.java com/tencent/mm/opensdk/modelbiz/WXNontaxPay.java com/tencent/mm/opensdk/modelbiz/WXOpenBusinessView.java com/tencent/mm/opensdk/modelbiz/WXPayInsurance.java com/tencent/mm/opensdk/modelbiz/WXPreloadMiniProgram.java com/tencent/mm/opensdk/modelmsg/GetMessageFromWX.java com/tencent/mm/opensdk/modelmsg/LaunchFromWX.java com/tencent/mm/opensdk/modelmsg/SendAuth.java com/tencent/mm/opensdk/modelmsg/SendMessageToWX.java com/tencent/mm/opensdk/modelmsg/WXApp

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ExtendObject.java com/tencent/mm/opensdk/modelmsg/WXDesignerSharedObject.java com/tencent/mm/opensdk/modelmsg/WXDynamicVideoMiniProgramObject.java com/tencent/mm/opensdk/modelmsg/WXEmojiObject.java com/tencent/mm/opensdk/modelmsg/WXEmojiPageSharedObject.java com/tencent/mm/opensdk/modelmsg/WXEmojiSharedObject.java com/tencent/mm/opensdk/modelmsg/WXEnterpriseCardObject.java com/tencent/mm/opensdk/modelmsg/WXFileObject.java com/tencent/mm/opensdk/modelmsg/WXGameVideoFileObject.java com/tencent/mm/opensdk/modelmsg/WXImageObject.java com/tencent/mm/opensdk/modelmsg/WXLiteAppObject.java com/tencent/mm/opensdk/modelmsg/WXMediaMessage.java com/tencent/mm/opensdk/modelmsg/WXMiniProgramObject.java com/tencent/mm/opensdk/modelmsg/WXMusicObject.java com/tencent/mm/opensdk/modelmsg/WXMusicVideoObject.java com/tencent/mm/opensdk/modelmsg/WXStateJumpChannelProfileInfo.java com/tencent/mm/opensdk/modelmsg/WXStateJumpMiniProgramInfo.java com/tencent/mm/opensdk/modelmsg/WXStateJumpUrlInfo.java com/tencent/mm/opensdk/modelmsg/WXStateSceneDataObject.java com/tencent/mm/opensdk/modelmsg/WXTextObject.java com/tencent/mm/opensdk/modelmsg/WXVide

NO	ISSUE	SEVERITY	STANDARDS	FILES
				oFileObject.java com/tencent/mm/opensdk/modelmsg/WXVideoObject.java com/tencent/mm/opensdk/modelmsg/WXWebpageObject.java com/tencent/mm/opensdk/modelpay/PayReq.java com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java com/tencent/mm/opensdk/openapi/MMSharedPreferences.java com/tencent/mm/opensdk/openapi/WXAPIFactory.java com/tencent/mm/opensdk/openapi/WXApiImplComm.java com/tencent/mm/opensdk/utils/Log.java com/tencent/mm/opensdk/utils/b.java defpackage/a230.java defpackage/a4a0.java defpackage/a92.java defpackage/aan.java defpackage/adm.java defpackage/ae.java defpackage/ae20.java defpackage/af20.java defpackage/ahy.java defpackage/ai3.java defpackage/ako.java defpackage/alr.java defpackage/an90.java defpackage/anw.java defpackage/aok.java defpackage/aqb.java defpackage/atd.java defpackage/aui.java defpackage/ax50.java defpackage/ayn.java defpackage/b0a0.java defpackage/b2k.java defpackage/b4a0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/b4d.java defpackage/bcl.java defpackage/be80.java defpackage/bh40.java defpackage/bha0.java defpackage/bih.java defpackage/blv.java defpackage/bpa0.java defpackage/bpe.java defpackage/bq2.java defpackage/bta0.java defpackage/bu30.java defpackage/bui.java defpackage/bw80.java defpackage/bww.java defpackage/byi.java defpackage/c1i.java defpackage/c1y.java defpackage/c320.java defpackage/c5a0.java defpackage/c7w.java defpackage/c91.java defpackage/caf.java defpackage/cai.java defpackage/cl30.java defpackage/clv.java defpackage/cm40.java defpackage/cmn.java defpackage/csk.java defpackage/d160.java defpackage/d2k.java defpackage/d39.java defpackage/d7a0.java defpackage/d810.java defpackage/d9i.java defpackage/dc4.java defpackage/ddq.java defpackage/dg6.java defpackage/dl40.java defpackage/dll.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/dmg.java defpackage/dmm.java defpackage/doe.java defpackage/dpv.java defpackage/dw80.java defpackage/dx90.java defpackage/dzj.java defpackage/e060.java defpackage/e14.java defpackage/e1y.java defpackage/e230.java defpackage/e3l.java defpackage/e4a.java defpackage/e6a.java defpackage/e7h.java defpackage/ec4.java defpackage/ecg.java defpackage/ee9.java defpackage/ek80.java defpackage/ell.java defpackage/emz.java defpackage/epl.java defpackage/eq9.java defpackage/ew80.java defpackage/eyi.java defpackage/f260.java defpackage/f2m.java defpackage/f3l.java defpackage/f4a.java defpackage/f66.java defpackage/f720.java defpackage/f7h.java defpackage/fdl.java defpackage/fe4.java defpackage/fjo.java defpackage/fk90.java defpackage/fm0.java defpackage/fm90.java defpackage/fn90.java defpackage/fnb.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	defpackage/fpv.java defpackage/fqz.java defpackage/fsd.java defpackage/fsu.java defpackage/fu1.java defpackage/fuq.java defpackage/fvd.java defpackage/fvt.java defpackage/fyi.java defpackage/fyj.java defpackage/g1a0.java defpackage/g1e.java defpackage/g4a.java defpackage/g5s.java defpackage/g9i.java defpackage/gaf.java defpackage/gd90.java defpackage/gf80.java defpackage/gg90.java defpackage/ghy.java defpackage/gi.java defpackage/gk80.java defpackage/gm90.java defpackage/gne.java defpackage/gww.java defpackage/h160.java defpackage/h1e.java defpackage/h3n.java defpackage/h700.java defpackage/h9n.java defpackage/ha0.java defpackage/hbl.java defpackage/hf80.java defpackage/hgh.java defpackage/hhy.java defpackage/hi.java defpackage/hl00.java defpackage/hlc.java defpackage/hoe.java defpackage/hor.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/hpc.java defpackage/hs0.java defpackage/hu90.java defpackage/hum.java defpackage/hx80.java defpackage/hyn.java defpackage/hz90.java defpackage/i0a0.java defpackage/i890.java defpackage/i92.java defpackage/ihc.java defpackage/ihy.java defpackage/ijm.java defpackage/il80.java defpackage/iy80.java defpackage/j940.java defpackage/j9f.java defpackage/jai.java defpackage/jb30.java defpackage/jcg.java defpackage/jg7.java defpackage/jgg.java defpackage/jj2.java defpackage/jjv.java defpackage/jw80.java defpackage/jyw.java defpackage/k28.java defpackage/k8f.java defpackage/kae.java defpackage/kbl.java defpackage/kpv.java defpackage/kq90.java defpackage/kra0.java defpackage/kva0.java defpackage/kvm.java defpackage/ky50.java defpackage/l0b.java defpackage/l160.java defpackage/l230.java defpackage/l29.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/l5h.java defpackage/lbl.java defpackage/lh90.java defpackage/lhy.java defpackage/lj80.java defpackage/ls00.java defpackage/ltd.java defpackage/ltw.java defpackage/lvt.java defpackage/m790.java defpackage/m9i.java defpackage/maf.java defpackage/mbl.java defpackage/mcc.java defpackage/mgj.java defpackage/mgy.java defpackage/mh.java defpackage/mk90.java defpackage/mps.java defpackage/ms00.java defpackage/mu10.java defpackage/mu90.java defpackage/muk.java defpackage/mvm.java defpackage/n48.java defpackage/n6h.java defpackage/n8f.java defpackage/naf.java defpackage/ncm.java defpackage/nd90.java defpackage/nf30.java defpackage/ngi.java defpackage/nh90.java defpackage/nix.java defpackage/njd.java defpackage/no90.java defpackage/npg.java defpackage/nv90.java defpackage/o5m.java defpackage/o690.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/oc00.java defpackage/od.java defpackage/of30.java defpackage/oio.java defpackage/ok30.java defpackage/op90.java defpackage/ow00.java defpackage/ow50.java defpackage/oy7.java defpackage/oyj.java defpackage/p030.java defpackage/p1l.java defpackage/p1x.java defpackage/p4.java defpackage/p56.java defpackage/p710.java defpackage/pj20.java defpackage/pkn.java defpackage/pm40.java defpackage/psu.java defpackage/pt40.java defpackage/ptg.java defpackage/pv0.java defpackage/px90.java defpackage/py50.java defpackage/q260.java defpackage/q29.java defpackage/q510.java defpackage/q56.java defpackage/q690.java defpackage/q81.java defpackage/qb2.java defpackage/qbc.java defpackage/qbl.java defpackage/qc00.java defpackage/qcg.java defpackage/qga0.java defpackage/qka0.java defpackage/qm90.java defpackage/qpy.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/qq90.java defpackage/qv0.java defpackage/qva.java defpackage/qxa.java defpackage/r090.java defpackage/r1x.java defpackage/r3d.java defpackage/r56.java defpackage/r6v.java defpackage/r81.java defpackage/r91.java defpackage/rf90.java defpackage/rh.java defpackage/rh3.java defpackage/rh80.java defpackage/ri3.java defpackage/rk30.java defpackage/rp2.java defpackage/rpa.java defpackage/rpc.java defpackage/rqn.java defpackage/rs30.java defpackage/rua.java defpackage/rxw.java defpackage/rya.java defpackage/s11.java defpackage/s1x.java defpackage/sj20.java defpackage/sk30.java defpackage/sn.java defpackage/sp90.java defpackage/spg.java defpackage/sqz.java defpackage/srg.java defpackage/sx90.java defpackage/sz90.java defpackage/t030.java defpackage/t090.java defpackage/t4.java defpackage/t56.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/tal.java defpackage/tgy.java defpackage/tix.java defpackage/tk30.java defpackage/tn0.java defpackage/tn90.java defpackage/tqa.java defpackage/ttc.java defpackage/u030.java defpackage/u1x.java defpackage/u690.java defpackage/u6f.java defpackage/u8n.java defpackage/ud.java defpackage/uf9.java defpackage/ui90.java defpackage/uia0.java defpackage/uj80.java defpackage/ukk.java defpackage/ume.java defpackage/un20.java defpackage/uo2.java defpackage/uoi.java defpackage/uov.java defpackage/uqa.java defpackage/uqe.java defpackage/uqz.java defpackage/utg.java defpackage/uu50.java defpackage/v0k.java defpackage/v5g.java defpackage/v91.java defpackage/vaf.java defpackage/vh30.java defpackage/vo8.java defpackage/vov.java defpackage/vq8.java defpackage/vu1.java defpackage/vu90.java defpackage/vw50.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/w03.java defpackage/w56.java defpackage/w690.java defpackage/w790.java defpackage/w8n.java defpackage/wb90.java defpackage/wd20.java defpackage/wo60.java defpackage/wo8.java defpackage/wpe.java defpackage/wru.java defpackage/wv10.java defpackage/wx90.java defpackage/wz8.java defpackage/x790.java defpackage/xa90.java defpackage/xd.java defpackage/xf90.java defpackage/xfb.java defpackage/xja0.java defpackage/xk30.java defpackage/xlt.java defpackage/xp2.java defpackage/xrg.java defpackage/xs1.java defpackage/xta0.java defpackage/xz80.java defpackage/y6h.java defpackage/ya90.java defpackage/yja0.java defpackage/yjn.java defpackage/ys00.java defpackage/yu20.java defpackage/yua0.java defpackage/yx90.java defpackage/yz90.java defpackage/z.java defpackage/z4a.java defpackage/z710.java defpackage/z8e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/z92.java defpackage/zf7.java defpackage/zit.java defpackage/zja0.java
				defpackage/zm00.java defpackage/zo2.java defpackage/zoa0.java defpackage/zsa0.java defpackage/ztf.java defpackage/zt8.java defpackage/zx0.java defpackage/zy90.java defpackage/zyh.java fwfd/com/fwfsdk/util/FWFLogger.java io/sentry/android/core/e.java io/sentry/android/core/f.java com/adjust/sdk/Constants.java com/adjust/sdk/sig/KeystoreHelper.java com/appboy/enums/CardKey.java com/deliveryhero/auth/ageverification/openid/OpenIdAuthUrlApiResponse.java com/deliveryhero/chatsdk/util/PushNotificationParser.java com/deliveryhero/cobrandedcard/common/data/model/CoBrandedErrorModel.java com/deliveryhero/cobrandedcard/issuance/data/remote/model/issuance/IssuanceSuccessResponse.java com/deliveryhero/configs/api/VariationInfo.java com/deliveryhero/configs/featuretoggle/MissingVariationKeyException.java com/deliveryhero/contract/model/PhoneCallType.java com/deliveryhero/corporate/data/entity/response/allowance/my/MyAllowanceOnBoardingItemResponse.java com/deliveryhero/dinein/data/api/models/rdp/VendorDineInDetailsApiModel.java com/deliveryhero/dinein/data/api/models/rnr/VendorReviewsApiModel.java com/deliveryhero/dinein/presentation/gallery/DineInGalleryComposeActivity.java com/deliveryhero/fintech/payments/card/configuration/data/models/EncryptionKeyApiModel.java com/deliveryhero/fintech/payments/card/encryption/EncryptionError.java com/deliveryhero/fwf_client/model/ProtoFeatureMsg.java com/deliveryhero/fwf_http/model/FeatureRequest.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/deliveryhero/grouporder/root/c.java com/deliveryhero/homescreen/container/navigation/i.java com/deliveryhero/location/presentation/address/coordinator/l.java com/deliveryhero/pandago/data/exceptions/PandaGoPaymentConfirmIntentApiErrorModel.java com/deliveryhero/pandago/data/model/DynamicError.java com/deliveryhero/pandago/data/model/DynamicText.java com/deliveryhero/pandago/data/model/ScheduleDeliveryCategoryApiModel.java com/deliveryhero/pandago/data/model/TrackingEtaApiModel.java com/deliveryhero/payment/cashier/h.java com/deliveryhero/payment/paymentselector/integrations/InstrumentPublicFieldsApiModel.java com/deliveryhero/payment/paymentselector/integrations/MetaDataApiModel.java com/deliveryhero/payment/paymentselector/integrations/PaymentDetailsApiModel.java com/deliveryhero/payment/paymentselector/integrations/checkout/cashback/CashbackResponsesApiModel.java com/deliveryhero/payment/paymentselector/xendit/model/remote/CollectBankOfChoiceResponse.java com/deliveryhero/shop/details/data/config/GroceriesConfig.java com/deliveryhero/subscription/presentation/details/p.java com/deliveryhero/vendorinfo/data/remote/DynamicMapApiModel.java com/klarna/mobile/sdk/core/ui/dialog/DialogAbstraction.java com/tencent/mm/opensdk/constants/ConstantsAPI.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/a840.java defpackage/af7.java defpackage/ah7.java defpackage/ahf.java defpackage/aro.java defpackage/dbt.java defpackage/dci.java defpackage/dd30.java defpackage/f6o.java defpackage/g6a.java defpackage/hhm.java defpackage/hov.java defpackage/idd.java defpackage/j1q.java defpackage/j6r.java defpackage/jw6.java defpackage/kvv.java defpackage/l2z.java defpackage/lvv.java defpackage/lzx.java defpackage/mg7.java defpackage/mlh.java defpackage/n46.java defpackage/o2n.java defpackage/poc.java defpackage/pww.java defpackage/qh9.java defpackage/qnr.java defpackage/qp6.java defpackage/qtf.java defpackage/rin.java defpackage/rt10.java defpackage/rtd.java defpackage/rtp.java defpackage/srz.java defpackage/tbo.java defpackage/ts10.java defpackage/us10.java defpackage/v13.java defpackage/vn00.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/vx60.java defpackage/wso.java defpackage/wu4.java defpackage/y3d.java defpackage/y9u.java defpackage/yge.java defpackage/yq40.java defpackage/yrc.java defpackage/z740.java defpackage/z920.java defpackage/zgh.java defpackage/zja.java defpackage/zx3.java fwfd/com/fwfsdk/util/FWFHelper.java com/shakebugs/shake/internal/I.java
4	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	defpackage/b1x.java defpackage/bdx.java defpackage/cdx.java defpackage/ddx.java defpackage/df90.java defpackage/dn90.java defpackage/edx.java defpackage/f1x.java defpackage/fdx.java defpackage/gdx.java defpackage/hwa0.java defpackage/ie90.java defpackage/l1x.java defpackage/p1x.java defpackage/uaf.java defpackage/uia0.java defpackage/vw90.java defpackage/w2a0.java defpackage/z2a0.java defpackage/zm90.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	defpackage/e09.java defpackage/ero.java defpackage/f190.java defpackage/g5s.java defpackage/ir3.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	bo/app/a0.java bo/app/a5.java bo/app/c6.java bo/app/e.java bo/app/e1.java bo/app/j1.java bo/app/k0.java bo/app/k6.java bo/app/l.java bo/app/l0.java bo/app/l4.java bo/app/m.java bo/app/m0.java bo/app/n6.java bo/app/r1.java bo/app/t6.java bo/app/v3.java bo/app/x0.java com/klarna/mobile/sdk/core/io/assets/util/AssetsUtil.java com/shakebugs/shake/internal/r2.java defpackage/bh40.java defpackage/edl.java defpackage/kpy.java defpackage/l4.java defpackage/qnl.java defpackage/ris.java defpackage/rjt.java defpackage/th2.java defpackage/tnl.java defpackage/ugi.java defpackage/vyw.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	bo/app/a5.java bo/app/k0.java bo/app/k6.java bo/app/n6.java bo/app/o5.java bo/app/p5.java bo/app/x0.java bo/app/y4.java defpackage/p0a0.java
8	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	com/deliveryhero/helpcenter/ui/HelpCenterActivity.java com/deliveryhero/subscription/presentation/webview/SubscriptionWebViewFragment.java defpackage/jai.java defpackage/mmr.java org/mp4parser/boxes/iso14496/part12/MediaDataBox.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	defpackage/a4a0.java defpackage/nz80.java defpackage/vz90.java defpackage/yww.java defpackage/zsa0.java io/sentry/android/core/internal/util/k.java io/sentry/android/core/s0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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	com/shakebugs/shake/internal/domain/models/deviceinfo/DeviceInfo.java com/shakebugs/shake/internal/utils/FileProvider.java defpackage/i3p.java defpackage/jai.java defpackage/jm40.java defpackage/qae.java defpackage/vbl.java defpackage/yk6.java io/sentry/android/core/s0.java
11	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/shakebugs/shake/network/ShakeNetworkInterceptor.java
12	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	com/deliveryhero/dinein/presentation/tabsquare/voucherdetails/c.java com/deliveryhero/pandago/ui/order/OrderTrackingFragment.java defpackage/ks0.java defpackage/tp30.java defpackage/u8s.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
13	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	com/deliveryhero/evaluation/yuu/pairing/YuuPairingActivity.java com/deliveryhero/helpcenter/ui/HelpCenterActivity.java com/deliveryhero/loyalty/pairing/LoyaltyPairingActivity.java com/deliveryhero/ordertracker/donation/a.java com/deliveryhero/payment/paymentselector/creditcard/webview/AddCreditCardActivity.java com/klarna/mobile/sdk/core/ui/dialog/internalbrowser/BaseInternalBrowserDialogFragment.java defpackage/arl.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	defpackage/dmg.java defpackage/fy0.java defpackage/k66.java defpackage/m9i.java defpackage/nz80.java io/sentry/t.java
15	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	com/tencent/mm/opensdk/channel/a/a.java defpackage/f7h.java defpackage/gj90.java defpackage/kic.java defpackage/lt90.java defpackage/mt00.java defpackage/qka0.java defpackage/xt1.java
16	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
17	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	defpackage/ia0.java defpackage/ny9.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/24	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.VIBRATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.READ_CONTACTS, android.permission.CAMERA, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.READ_PHONE_STATE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	5/45	android.permission.READ_CALENDAR, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:
Permissions that are commonly abused by known malware.

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://android-foodora.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
support@avo.app	defpackage/cm40.java
u0013android@android.com0 u0013android@android.com	defpackage/d4a0.java
android@foodora.com	defpackage/elz.java
fdapac_header_img@3x.png	defpackage/oqy.java
android@foodora.com	defpackage/uqe.java

EMAIL	FILE
support@foodora.it corporate@foodpanda.com name@email.com support@foodpanda.sg support@foodora.no corporate@foodpanda.sg name@company.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
Braze (formerly Appboy)	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/17
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

HARDCODED SECRETS

POSSIBLE SECRETS

"NEXTGEN_ACNT_PASSWORD" : "Password"

"NEXTGEN_DINEIN_PAYMENT_CANCEL_AUTH_DIALOG_CTA" : "Cancel"

"NEXTGEN_LOGIN_SHOW_PASSWORD" : "Show"

"NEXTGEN_REGISTER_STARTED_SHOW_PASSWORD" : "Show"

"NEXTGEN_SUBS_RP_SCPWD_INFO_FOOTER_BACK_CTA" : "Back"

"PXServerToken" : "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzY29wZXMiOlsicmlza19zY29yZSIsInJlc3RfYXBpIl0sImlhdCI6MTYxMjE3NjkxNiwic3ViIjoiUFh6ZTNuQzNPcyIsImp0aSI6IjJhMWQyZjUxLTg1ZDAtNGI0MC1hMDAxLWQwZmU2MzIzZWMxNyJ9.O8OEZqDESrC4f6IXD84MY4XmbpskGcAOjjKKrgKBYLQ"

"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"

"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"

"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"

"file_provider_authority" : "com.global.foodpanda.android.fileprovider"

"firebase_database_url" : "https://android-foodora.firebaseio.com"

"google_api_key" : "AIzaSyCdrhSSqNXjpXEMEzXXTeSige--1ZV9DoM"

"google_crash_reporting_api_key" : "AIzaSyCdrhSSqNXjpXEMEzXXTeSige--1ZV9DoM"

"library_fastadapter_authorWebsite" : "http://mikepenz.com/"

"library_materialize_authorWebsite" : "http://mikepenz.com/"

POSSIBLE SECRETS
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"shared_prefs_app_id_key_klarna_inapp_sdk" : "sdk-application-id"
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
8bd31fecc28e51e25119c9342c6c3a1c
e2eaf828d1423fe9372478b0cc9ddba721042797ef4d76525c364ec1e0c5832c
97be66c02ec53eb4ab7d6d4ea2e17633
37a6259cc0c1dae299a7866489dff0bd
c56fb7d591ba6704df047fd98f535372fea00211
dQM6X4cPRCBSMmRGMtiy6orUJKVAsgHWiEX4eeQBvYqNvUV2IqrJl7C6
7c43a395daac2b34160a23226813afc0
a8b5894279328d2a82e72f1a7dded823e00f68c02103c49eaaecf1c4cf5a1c48
b58f86f3ec0a4a14d230344fd2c6d7a16dd7ecf10b042ba1bcc97b31996b1621
sha256/grX4Ta9HpZx6tSHkmCrvpApTQGo67CYDnvprLg5yRME=
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
b79e65184ce0257bef861190ae475cc7

POSSIBLE SECRETS
eb69a8f19dafdd26fce238e28a02faa4fb0c3d05bf36732afa3e69cd3f2d4e82
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
c08775fa34cef6ab7d6d6fe1bc651f6c7a3bc6ff8ea929cf33f6e834f7919c87
71a06dcaefd3b757f5fd464881f7b0014daf7d098c9986307ef872e80492edd5
7f64ad933e215a49af9586df4f2d602c2277145e2d6b0721b22f593b334d268b
39a19a315fe143742044c49a1116bea5
38ee6f60cc59261c404d38c7413f23159b5896eac4f554d88b91de0b60bcc869
T7tlPcyTHtFZ8W0qAEV56Wgj6PL2T6DG
fXoQtIbGcN0zkVYtS7g9hL2bl1gPiczbsl
d8f72b07e66444b8d3e07af9d97b963eae3682f482c5de5d84f25bca02dc7862
9b8f518b086098de3d77736f9458a3d2f6f95a37
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
758a7ad79beb3aa2b49da038718c1ada
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
4f85e88ff3c25eb6c71a99742db2679fc5026183bc7ddbd24cba073747c92a35

POSSIBLE SECRETS
fb8760f8-6ffc-466a-8d98-0a9b4584e07a
62b3abd864bde7488eae5ff575b51091f2d2b929f1d178fbed01c593ed62794e
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
400f56d2814c03e05eb53452e852464d
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
9A04F079-9840-4286-AB92-E65BE0885F95
8G3ZKFzAnqZbNurKqIN9mX5amqQFq5sQXFWF2Nlk
AGpgvYFRN6oWceHKF2MtDZzXGbivkqKj38mNRZ
4d419a24ce2f37cd74ef818f728a1979d39ed57f4380f41cff6f6f6f7d5e133c
91922a0275b018d572b693dd854bee64e9794a944a95364d9542a59a09e8d013
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
61a76bbf38102fa61a8f51b6181dc18c
310aaee6497180a238ecf313d7787ef26c0fadf3fd48d0dc75fb7c873ad1987f

POSSIBLE SECRETS
629d19195e0bf14d54e871429df31066a917f7c4b8931c39e199edcad8a8a740
af506cb579a77e20f1c238c0afeab5a8715ea01e05f5e9c8d8a16beab389f6da
09a5a04de61bb3ba50f7f4b03bee3579
115792089210356248762697446949407573529996955224135760342422259061068512044369
0123456789abcdefABCDEF
3f6bb38af3b343e95f092ebe5173a343
94743e275c3fcfce8bc483b591df18c0
c2ee647e9689dae80722aa39023f79a8
c103703e120ae8cc73c9248622f3cd1e
87c5a9e33a1556cefbaf04b18841e0e6172a40dbeb86b8dc1bf75e73991959a7
20106998-7fd6-4e1c-9f5d-f66d7fb6cd21
A2B55680-6F43-11E0-9A3F-0002A5D5C51B
1Fn28Ziqh6NbpfE422YhL3kXTQ5yC4cgtQsqSvfmHWgi4WjLH301xEx
b837020d1626632d838e12ec107f2897
ed1e1c6cf50e562eccfc6e353eb023e481c1c701ab69c3fa66f5e9d44c5ae9ca

POSSIBLE SECRETS
cc2751449a350f668590264ed76692694a80308a
a029a18ff8b1a86fcc01b35351569668
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
8def219c54b8b02bb9afae8298c9011d980400e78cb46784d64c3d4ebe33cce8
b612e6f61a58f6d2e3c71638e55d39ee6a94247eba970a1788715d3e31a6e049
2b5d6657437fd523698792e70bb6f8ee45a6a0bb82217eb9f49aed9bd8dc6cb6
790646be452ec5050b65785c33d02e3e4d4fbec581b4ed2c257f3c4ae177699f
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
58b246d4-99aa-4438-a1cd-967602c7fcbb
30820268308201d102044a9c4610300d06092a864886f70d0101040500307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b13084661636562656f6f6b311d301b060355040313144661636562656f6f6b20436f72706f726174696f6e3020170d3039303833313231353231365a180f32303530303932353231353231365a307a310b3009060355040613025553310b3009060355040813024341311230100603550407130950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b13084661636562656f6f6b311d301b060355040313144661636562656f6f6b20436f72706f726174696f6e30819f300d06092a864886f70d010101050003818d00308189028181100c207d51df8eb8c97d93ba0c8c1002c928fab00dc1b42fca5e66e99cc3023ed2d214d822bc59e8e35ddcf5f44c7ae8ade50d7e0c434f500e6c131f4a2834f987fc46406115de2018ebbb0d5a3c261bd97581ccfef76afc7135a6d59e8855ecd7eacc8f8737e794c60a761c536b72b11fac8e603f5da1a2d54aa103b8a13c0dbc10203010001300d06092a864886f70d0101040500038181005ee9be8bcbb250648d3b741290a82a1c9dc2e76a0af2f2228f1d9f9c4007529c446a70175c5a900d5141812866db46be6559e2141616483998211f4a673149fb2232a10d247663b26a9031e15f84bc1c74d141ff98a02d76f85b2c8ab2571b6469b232d8e768a7f7ca04f7abe4a775615916c07940656b58717457b42bd928a2
82213c1f-c715-4970-bec9-5f48fea42e7d
565d4106-3c24-4f57-9435-aea2f44f675e

POSSIBLE SECRETS
sha256/V5L96iSCz0XLFgvKi7YVo6M4SIkOP9zSkDjZ0EoU6b8=
1603907e3186ad7b6cc1183f7eaf1f7c364c90e6d26827955b51fabf8b5d675c
7e7b6b9433a233b86855e980acbe0689
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
eaeb85e7f91d49f6272f9cdf52d270d13cfb754f08559ab3e1641490f1840467
29d3d13e441296535c55aa9ef241403e
4316db3f7e84e285ad46c9fc67c22312
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
c9d6ab7e60369098acfea58dd81d22c9
8fc33759f3362c37e237950fd213aec913a2542bb4ff0f0dc47feb6def6d110d
0e8b7dcd3078579ac5da1020bcd854d800c12f6587a397ef92b6751a8cfdb041
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
eacd05ddef02e59c683725a264c61b3346180e1a318fbed3e3ae1f493069d53c

POSSIBLE SECRETS
49f946663a8deb7054212b8adda248c6
308202eb30820254a00302010202044d36f7a4300d06092a864886f70d01010505003081b9310b3009060355040613023836311230100603550408130947756 16e67646f6e673111300f060355040713085368656e7a68656e3135303306035504 0a132c54656e63656e7420546563686e6f6c6f6779285368656e7a68656e292043 6f6d70616e79204c696d69746564313a3038060355040b133154656e63656e74204775616e677a686f752052657365617263682061 6e6420446576656c6f706d656e742043656e7465723110300e060355040313075 4656e63656e74301e170d313130313139313433393332 5a170d343130313131313433393332 5a3081b9310b3009060355040613023836311230100603550408130947756 16e67646f6e673111300f060355040713085368656e7a68656e3135303306035504 0a132c54656e63656e7420546563686e6f6c6f6779285368656e7a68656e2920436f6d70616e79204c696d69746564313a3038060355040b133154656e63656e74204775616e677a 686f752052657365617263682061 6e6420446576656c6f706d656e742043656e7465723110300e060355040313075 4656e63656e7430819f300d06092a864886f7 0d010101050003818d0030818902818100c05f34b231b083fb1323670bfbe7bdab40c0c0a6efc87ef2072a1ff0d60cc67c8edb0d0847f210bea6cbfaa241be70c86daf5 6be08b723c859e52428a064555d80db448cdcacc1aea2501eba06f8bad12a4fa49d85cacd7abeb68945a5cb5e061629b52e3254c373550ee4e40cb7c8ae6f7a8151ccd 8df582d446f39ae0c5e930203010001300d06092a864886f70d01010505000381810 09c8d9d7f2f908c42081b4c764c377109a8b2c70582422125ce545842d5f520ae a69550b6bd8bfd94e987b75a3077eb04ad341f481aac266e89d3864456e69fba13df018acdc168b9a19dfd7ad9d9cc6f6ace57c746515f71234df3a053e33ba93ece5cd 0fc15f3e389a3f365588a9fcb439e069d3629cd7732a13fff7b891499
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
5a8ed0ef41beb6f1c986b48280b02d69
c8e43223c4bd4020eba83d17abe4470d
F4Po0h6zvJpwrMet5GnLdwlhgHpD6x8ceNI3SwXvBw2IljkPaKmKSrunalySrx5nSvfLULENmARYkxSxhwrglt2Mhe057
NUcUDJtM2Z6GuQQnG4PordFwXDdLWQo3FjDubsMUmcwQi3U8s
87a98ea95a4753e4491a35143a2b5a350358fdfab519e76ee618d05c15bf0d11
299ad2ea59fc2559f88e945a178f6cdec5edaa9ddfe9514f7993719b83fff696
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449

POSSIBLE SECRETS
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00

PLAYSTORE INFORMATION

Title: foodpanda: food & groceries

Score: 4.0229883 **Installs:** 100,000,000+ **Price:** 0 **Android Version Support:** **Category:** Food & Drink **Play Store URL:** com.global.foodpanda.android

Developer Details: Foodpanda GmbH a subsidiary of Delivery Hero SE, Foodpanda+GmbH+a+subsidiary+of+Delivery+Hero+SE, None, https://www.foodpanda.com/, appsupport@foodpanda.com,

Release Date: Nov 19, 2013 **Privacy Policy:** Privacy link

Description:

live like a panda You do you, we'll bring food and groceries in a flash. In the mood for comfort food from your fave restaurant? Dreading another grocery trip? Spend time doing things you love, we'll take care of your meals with the best deals. Food for your cravings. Hungry for wood-fired pizza, a classic burger or fried chicken? We know the best restaurants near you – big famous brands and tiny local faves. Best part? We've got exclusive discounts and promos waiting for all new foodies. Fresh groceries in a flash. Skip that grocery trip. We'll do the heavy lifting. Get groceries, snacks and drinks fast from pandamart and foodpanda shops. We deliver fresh produce, essentials, frozen goods, personal care items, your cute pet's needs and much more. Save on tasty takeaways. On the go? Try pick-up! Skip the queue and save up when you self-collect your order. Worry-free package delivery. Need to send or receive a parcel? Go with pandago. Our reliable fleet will safely deliver it for you in no time. What makes us special? We get you. There's no time to waste waiting. Pick what you love and we'll bring it in a tap. Save your go-to places and reorder faves with ease. Want more? Become a pro and save big on your yummy orders. Our tech is shaped by you. Explore personalised offers and delicious picks just for you. Dish out what you feel about your order and let foodies know what's yum. For more info, visit https://www.foodpanda.com.bd/ https://www.foodpanda.hk/ https://www.foodpanda.com.kh/ https://www.foodpanda.la/ https://www.foodpanda.com.mm/ https://www.foodpanda.my/ https://www.foodpanda.ph/ https://www.foodpanda.pk/ https://www.foodpanda.sg/ https://www.foodpanda.co.th/ https://www.foodpanda.com.tw/
