



ANDROID STATIC ANALYSIS REPORT



 BuzzRx (177.0)

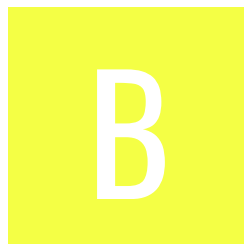
File Name: io.pdcgs.buzzrxconsumer_177.apk

Package Name: io.pdcgs.buzzrxconsumer

Scan Date: Sept. 1, 2025, 1:59 p.m.






App Security Score: 46/100 (MEDIUM RISK)

Grade:



Trackers Detection: 4/432

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
3	22	1	1	1

FILE INFORMATION

File Name: io.pdcgs.buzzrxconsumer_177.apk

Size: 14.92MB

MD5: 4fc2fe80c16b442418dfcc38232a34ca

SHA1: ec85742e2266a0561caaf367c0e6551c646b6db4

SHA256: 212eff3783ed639cf40e7917946cdebde20c3e2da7a8a24d890f843b101a2ac8

APP INFORMATION

App Name: BuzzRx

Package Name: io.pdcgs.buzzrxconsumer

Main Activity: io.pdcgs.buzzrxconsumer.MainActivity

Target SDK: 34

Min SDK: 22

Max SDK:

Android Version Name: 177.0

Android Version Code: 177

APP COMPONENTS

Activities: 7

Services: 13

Receivers: 16

Providers: 3

Exported Activities: 3

Exported Services: 1

Exported Receivers: 7

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: True

v2 signature: True

v3 signature: True

v4 signature: False

X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2020-10-14 18:40:44+00:00

Valid To: 2050-10-14 18:40:44+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0x81ffe5819952a4184e62a7530c1b1b0fb7d6dc5

Hash Algorithm: sha256

md5: 7557741c6a85cee03686b2fbc880e21c

sha1: 5433f21ce894ac7f987fd3db9c209522aec2b569

sha256: 2e435f77585dd43b008f660a6a1651bd58f040f8b84e5bddb171a4762472acb8

sha512: fc36374a4f787dab73b8e4a899579ef10e0b9163656d638e2b721c09070690c89d4b3c733c4dd0218c53b879c1a66e66ae946d2a9b267dde9099ffed503475a4

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 3301abcc8c066a966bd2c05be64f931085d282f6a35cea3e67705fda79fd156e

Found 1 unique certificates

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
io.pdcgs.buzzrxconsumer.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
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.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.

PERMISSION	STATUS	INFO	DESCRIPTION
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_AD SERVICES_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.
com.samsung.android.mapsagent.permission.READ_APP_INFO	unknown	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
io.pdcgs.buzzrxconsumer.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

FILE	DETAILS	
4fc2fe80c16b442418dfcc38232a34ca.apk	FINDINGS	DETAILS
	Anti-VM Code	possible VM check
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check network operator name check ro.hardware check ro.kernel.qemu check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)

FILE	DETAILS	
classes2.dex	FINDINGS	DETAILS
	Anti Debug Code	Debug.isDebuggerConnected() check
	Anti-VM Code	Build.MODEL check Build.PRODUCT check possible Build.SERIAL check
	Compiler	r8 without marker (suspicious)
classes3.dex	FINDINGS	DETAILS
	Compiler	unknown (please file detection issue!)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
io.pdcgs.buzzrxconsumer.MainActivity	Schemes: @string/custom_url_scheme://, https://, buzzrxapp://, Hosts: buzzrx-app.onelink.me,

NETWORK SECURITY

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: 2 | WARNING: 13 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.1-5.1.1, [minSdk=22]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
4	Broadcast Receiver (com.onesignal.notifications.receivers.FCMBroadcastReceiver) 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.
5	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityHMS) 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
6	Broadcast Receiver (com.onesignal.notifications.receivers.NotificationDismissReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Broadcast Receiver (com.onesignal.notifications.receivers.BootUpReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Broadcast Receiver (com.onesignal.notifications.receivers.UpgradeReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Activity (com.onesignal.notifications.activities.NotificationOpenedActivity) 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	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityAndroid22AndOlder) 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.
11	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.

NO	ISSUE	SEVERITY	DESCRIPTION
12	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.
13	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.

NO	ISSUE	SEVERITY	DESCRIPTION
14	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.
15	High Intent Priority (999) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 6 | INFO: 1 | SECURE: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
----	-------	----------	-----------	-------

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	capacitor/plugin/appsflyer/sdk/AppsFlyerConstantsKt.java com/getcapacitor/AppUUID.java com/getcapacitor/Bridge.java com/getcapacitor/Plugin.java com/onesignal/inAppMessages/internal/display/impl/WebViewManager.java com/onesignal/inAppMessages/internal/prompt/InAppMessagePromptTypes.java com/onesignal/inAppMessages/internal/prompt/impl/InAppMessagePrompt.java com/onesignal/notifications/bridges/OneSignalHmsEventBridge.java com/onesignal/notifications/internal/Notification.java com/onesignal/notifications/internal/bundle/impl/NotificationBundleProcessor.java com/onesignal/notifications/internal/common/NotificationConstants.java com/onesignal/notifications/internal/common/NotificationHelper.java com/onesignal/notifications/receivers/FCMBroadcastReceiver.java uk/co/workingedge/phonegap/plugin/LaunchNavigatorPlugin.java
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/appsflyer/internal/AFb1bSDK.java com/appsflyer/internal/AFi1fSDK.java com/onesignal/common/AndroidUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/onesignal/core/internal/database/impl/OSDatabase.java com/onesignal/session/internal/outcomes/impl/OutcomeTableProvider.java
4	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	capacitor/plugin/appsflyer/sdk/AFHelpers.java com/appsflyer/internal/AFg1aSDK.java com/capacitorjs/plugins/network/NetworkPlugin.java com/getcapacitor/Logger.java com/getcapacitor/community/inappreview/InAppReview.java com/onesignal/debug/internal/logging/Logging.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/ShortcutBadger.java io/capawesome/capacitorjs/plugins/firebase/crashlytics/FirebaseCrashlytics.java uk/co/workingedge/phonegap/plugin/CordovaLogger.java uk/co/workingedge/phonegap/plugin/LaunchNavigatorPlugin.java
5	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/onesignal/inAppMessages/internal/display/impl/WebViewManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/onesignal/inAppMessages/internal/display/impl/WebViewManager.java
7	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/getcapacitor/BridgeWebChromeClient.java com/getcapacitor/FileUtils.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/getcapacitor/BridgeWebChromeClient.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
---------	-----------	-------	-------

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/appsflyer/internal/AFc1bSDK.java com/appsflyer/internal/AFc1kSDK.java com/appsflyer/internal/AFf1tSDK.java com/getcapacitor/Bridge.java com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/NavigateToAndroidSettingsForLocation.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/OPPOHomeBader.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SonyHomeBadger.java com/phonegap/plugins/nativesettings/NativeSettings.java uk/co/workingedge/LaunchNavigator.java
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFj1uSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFj1uSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1ISDK.java com/appsflyer/internal/AFj1uSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFj1tSDK.java com/appsflyer/internal/AFj1uSDK.java com/appsflyer/internal/AFj1vSDK.java com/appsflyer/internal/AFj1xSDK.java com/getcapacitor/FileUtils.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFj1uSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFj1uSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1ISDK.java com/appsflyer/internal/AFj1uSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java
00123	Save the response to JSON after connecting to the remote server	network command	com/getcapacitor/plugin/util/CapacitorURLConnection.java com/getcapacitor/plugin/util/HttpRequestHandler.java
00153	Send binary data over HTTP	http	com/getcapacitor/plugin/util/CapacitorURLConnection.java
00187	Query a URI and check the result	collection sms calllog calendar	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFj1tSDK.java com/appsflyer/internal/AFj1wSDK.java com/appsflyer/internal/AFj1xSDK.java com/getcapacitor/AndroidProtocolHandler.java com/getcapacitor/Bridge.java com/getcapacitor/plugin/util/AssetUtil.java com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/NavigateToAndroidSettingsForLocation.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/EverythingMeHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/HuaweiHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/NovaHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/OPPOHomeBader.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SonyHomeBadger.java com/onesignal/notifications/internal/common/NotificationHelper.java com/phonegap/plugins/nativesettings/NativeSettings.java
00096	Connect to a URL and set request method	command network	com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1ISDK.java com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/HttpRequestHandler.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1ISDK.java com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java
00109	Connect to a URL and get the response code	network command	com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1ISDK.java com/appsflyer/internal/AFf1kSDK.java com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/HttpRequestHandler.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFi1rSDK.java com/onesignal/common/DeviceUtils.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/NavigateToAndroidSettingsForLocation.java uk/co/workingedge/LaunchNavigator.java
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/AFb1rSDK.java com/appsflyer/internal/AFc1kSDK.java com/getcapacitor/Bridge.java com/onesignal/core/activities/PermissionsActivity.java com/onesignal/notifications/internal/common/NotificationFormatHelper.java com/onesignal/notifications/receivers/FCMBroadcastReceiver.java
00022	Open a file from given absolute path of the file	file	com/appsflyer/internal/AFg1jSDK.java com/getcapacitor/FileUtils.java com/getcapacitor/plugin/util/AssetUtil.java
00072	Write HTTP input stream into a file	command network file	com/getcapacitor/plugin/util/AssetUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java
00094	Connect to a URL and read data from it	command network	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java
00108	Read the input stream from given URL	network command	com/getcapacitor/WebViewLocalServer.java com/getcapacitor/plugin/util/AssetUtil.java com/getcapacitor/plugin/util/HttpRequestHandler.java
00013	Read file and put it into a stream	file	com/appsflyer/internal/AFa1ySDK.java com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFg1jSDK.java com/getcapacitor/AndroidProtocolHandler.java okio/Okio.java
00125	Check if the given file path exist	file	com/getcapacitor/Bridge.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1jSDK.java com/getcapacitor/FileUtils.java
00014	Read file into a stream and put it into a JSON object	file	com/appsflyer/internal/AFg1jSDK.java
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFg1jSDK.java
00028	Read file from assets directory	file	com/getcapacitor/FileUtils.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/274764693060/namespaces/firebase:fetch?key=AlzaSyBjYyFe-xyVACab-0Uhw5EHf5c_c1DbdVk . This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	5/44	android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
--------	----------------

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
sinapps.s	ok	No Geolocation information available.
citymapper.com	ok	IP: 141.101.90.105 Country: France Region: Ile-de-France City: Paris Latitude: 48.853409 Longitude: 2.348800 View: Google Map
share.here.com	ok	IP: 18.155.173.121 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
sdlSDK.s	ok	No Geolocation information available.
sconversions.s	ok	No Geolocation information available.
simpresion.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
smonitorsdk.s	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.
capacitorjs.com	ok	IP: 104.21.93.31 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
sattr.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
sars.s	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.
scdn-stestsettings.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
aps-webhandler.appsflyer.com	ok	IP: 18.238.109.53 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
api.onesignal.com	ok	IP: 104.16.160.145 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
maps.google.com	ok	IP: 216.58.207.238 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
sonelink.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
svalidate-and-log.s	ok	No Geolocation information available.
sapp.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
sviap.s	ok	No Geolocation information available.
svalidate.s	ok	No Geolocation information available.

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193

HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AlzaSyBjYyFe-xyVACab-0Uhw5EHf5c_c1DbdVk"
"google_crash_reporting_api_key" : "AlzaSyBjYyFe-xyVACab-0Uhw5EHf5c_c1DbdVk"
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F

POSSIBLE SECRETS
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
c682b8144a8dd52bc1ad63
5181942b9ebc31ce68dacb56c16fd79f
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
ae2044fb577e65ee8bb576ca48a2f06e
258EAF45-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcd9735803434cec591fa
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1

PLAYSTORE INFORMATION

Title: BuzzRx: Rx Local Drug Coupons

Score: 4.840708 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** [io.pdcgs.buzzrxconsumer](https://play.google.com/store/apps/details?id=io.pdcgs.buzzrxconsumer)

Developer Details: Buzz Group Holdings, Buzz+Group+Holdings, None, <https://buzzrx.com>, support@buzzrx.com,

Release Date: Oct 15, 2020 **Privacy Policy:** [Privacy link](#)

Description:

BuzzRx: Your Rx Savings Prescription Care Partner! Save on prescriptions with BuzzRx, the ultimate savings app for local Rx discounts. Need to save on prescription meds, at Walgreens, Walmart, CVS, Safeway, and Rite Aid? Or perhaps you need a prescription refill? BuzzRx has you covered! Navigate our Rx coupons to get unbeatable pharmacy discounts right in your neighborhood! Why BuzzRx? 1. Save on prescriptions: Find prescription discounts at Walgreens, Walmart, CVS, Rite Aid, and over 60,000 pharmacies nationwide. 2. Local Rx Discounts: Easily access local pharmacy discounts with our free coupons for meds. 3. Rx Coupons for Pets: Care for your furry friends with unbeatable Rx savings on their meds. 4. Prescription Refill: Stay on top of your prescriptions with our built-in medication reminder. Get BuzzRx now for incredible Rx

savings and enjoy great discounts on all your prescriptions at your local pharmacy! BuzzRx Features Prescription Discount Finder -Use our savings app to find the best Rx prices: -Enter your prescription Rx details and zip code. -Compare discounted Rx prices at pharmacies near you. -Redeem free Rx coupons by showing your BuzzRx card or coupon at checkout – no insurance required, and save up to 80% on prescriptions! Prescription Refill Reminder Never miss a dose! BuzzRx helps you stay organized with a personalized medication tracker and Rx medication reminder. Free Coupons for All Rx Medications Whether you have insurance or not, BuzzRx offers prescription discounts for every member of your family. Save on pet prescriptions, too! Accepted at 60,000+ Pharmacies BuzzRx partners with major pharmacy chains like: - CVS Pharmacy - Walmart Pharmacy - Walgreens Pharmacy - Rite Aid Pharmacy - Target Pharmacy - Safeway Pharmacy - Albertsons Pharmacy - Publix Pharmacy - Vons Pharmacy - Kroger Pharmacy - HEB Pharmacy - & much more! How It Works - Download BuzzRx and search for Rx savings on your prescription meds. - Use our pharmacy discount My Card or unlock Rx coupons for specific medications. - Redeem your savings and enjoy affordable prescriptions at any participating local Rx pharmacy. More Than Just Savings By using BuzzRx, you support charities like Make-A-Wish®, helping to create a positive impact while you save on prescriptions. Medication Tracker & Free Prescription Refill Reminder Never miss a prescription refill again with BuzzRx's handy reminder feature. Set a personalized Rx medication reminder to ensure you always have your medications on time, eliminating the stress of running out. We'll also keep you updated on the best Rx coupons and discounts available for your saved prescriptions. Redeem it at Your Local Pharmacy BuzzRx collaborates with over 60,000 pharmacies across the nation, including well-known names like CVS, Walgreens, Rite Aid, Kroger Pharmacy, Safeway Pharmacy, Walmart, and many more. Wherever you are, BuzzRx is there to help you save on prescriptions and enjoy affordable family care at your trusted pharmacy! BuzzRx: Your Prescription Discount Solution BuzzRx isn't just about saving on prescriptions—it's a comprehensive tool for managing your family's healthcare. With features like personalized Rx refill reminders and pharmacy price comparison, BuzzRx ensures you stay on top of your care. Whether it's finding the best local Rx pharmacy discount, saving on prescriptions for pets, or using free coupons to cut costs, BuzzRx is the ultimate Rx saver for all your healthcare needs. Take control of your well-being while saving money effortlessly. Affordable Rx care, local Rx savings, and more—all in one app. Save on prescriptions now! By downloading BuzzRx, you agree to be bound by our Terms of Use. Read more at <https://www.buzzrx.com/terms-of-use> Notice of Collection: <https://www.BuzzRx.com/California-Consumer-Privacy-Act-Privacy-Policy>

SCAN LOGS

Timestamp	Event	Error
2025-09-01 13:59:29	Generating Hashes	OK
2025-09-01 13:59:29	Extracting APK	OK
2025-09-01 13:59:29	Unzipping	OK

2025-09-01 13:59:29	Parsing APK with androguard	OK
2025-09-01 13:59:29	Extracting APK features using aapt/aapt2	OK
2025-09-01 13:59:29	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 13:59:30	Parsing AndroidManifest.xml	OK
2025-09-01 13:59:30	Extracting Manifest Data	OK
2025-09-01 13:59:30	Manifest Analysis Started	OK
2025-09-01 13:59:31	Performing Static Analysis on: BuzzRx (io.pdcgs.buzzrxconsumer)	OK
2025-09-01 13:59:33	Fetching Details from Play Store: io.pdcgs.buzzrxconsumer	OK
2025-09-01 13:59:34	Checking for Malware Permissions	OK
2025-09-01 13:59:34	Fetching icon path	OK
2025-09-01 13:59:34	Library Binary Analysis Started	OK

2025-09-01 13:59:34	Reading Code Signing Certificate	OK
2025-09-01 13:59:35	Running APKiD 2.1.5	OK
2025-09-01 13:59:38	Detecting Trackers	OK
2025-09-01 13:59:40	Decompiling APK to Java with JADX	OK
2025-09-01 13:59:53	Converting DEX to Smali	OK
2025-09-01 13:59:53	Code Analysis Started on - java_source	OK
2025-09-01 13:59:54	Android SBOM Analysis Completed	OK
2025-09-01 13:59:57	Android SAST Completed	OK
2025-09-01 13:59:57	Android API Analysis Started	OK
2025-09-01 14:00:00	Android API Analysis Completed	OK

2025-09-01 14:00:00	Android Permission Mapping Started	OK
2025-09-01 14:00:03	Android Permission Mapping Completed	OK
2025-09-01 14:00:03	Android Behaviour Analysis Started	OK
2025-09-01 14:00:06	Android Behaviour Analysis Completed	OK
2025-09-01 14:00:06	Extracting Emails and URLs from Source Code	OK
2025-09-01 14:00:07	Email and URL Extraction Completed	OK
2025-09-01 14:00:07	Extracting String data from APK	OK
2025-09-01 14:00:07	Extracting String data from Code	OK
2025-09-01 14:00:07	Extracting String values and entropies from Code	OK
2025-09-01 14:00:10	Performing Malware check on extracted domains	OK

2025-09-01 14:00:12	Saving to Database	OK
---------------------	--------------------	----

Report Generated by - MobSF v4.4.0

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.