ANDROID STATIC ANALYSIS REPORT

Alinma Bank (1.2.2)

File Name:	com.alinma.retail.mobile_10202_apps.evozi.com.apk
Package Name:	com.alinma.retail.mobile
Average CVSS Score:	6.9
App Security Score:	25/100 (HIGH RISK)
Trackers Detection:	2/405
Scan Date:	Sept. 28, 2021, 5:03 a.m.

FILE INFORMATION

File Name: com.alinma.retail.mobile_10202_apps.evozi.com.apk
Size: 18.36MB
MD5: 199f44453fe47ec7a4282642f4be2ae6
SHA1: c670231fa63e0aae245ae1a4dce0cb5186697fd2
SHA256: ade10eaecc3bcbfd9794fc0a333779a08718f842f6ac013ffdaae45604f2f602

APP INFORMATION

App Name: Alinma Bank
Package Name: com.alinma.retail.mobile
Main Activity: com.alinma.retail.mobile.MainActivity
Target SDK: 29
Min SDK: 19
Max SDK:
Android Version Name: 1.2.2
Android Version Code: 10202

APP COMPONENTS

Activities: 9
Services: 9
Receivers: 15
Providers: 8
Exported Activities: 0
Exported Services: 3
Exported Receivers: 5
Exported Providers: 1

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=009966, ST=Riyadh, L=Riyadh, O=Alinma Bank, OU=Alinma Bank, CN=Alinma Bank
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-04-02 11:38:03+00:00
Valid To: 2043-03-26 11:38:03+00:00
Issuer: C=009966, ST=Riyadh, L=Riyadh, O=Alinma Bank, OU=Alinma Bank, CN=Alinma Bank
Serial Number: 0x5f683e80
Hash Algorithm: sha256
md5: e1034f38956595fa198d2fb0541daf1f
sha1: 22fc4b7e17e1de8e0596ad90750de4c7c765e8e9
sha256: 4658c6ef9a946d7c19c79e74a13a6ce379eee8736a582e1e3206f7bed276a8d1
sha512:
ff8ed789c6f338069d1b9997c565b7aa8ffbefd57b17a1f7cf1c5a20c889828a32c65da7ba4b445619c786d0e3cc4d3a8dc1b45bb9b057556dafaebf6fca694c

PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: da0a38a40037faf6e78db1c54b47076620d4a88217a334e8e10447e945f7864c

STATUS	DESCRIPTION
secure	Application is signed with a code signing certificate
warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android <7.0

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
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.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
com.amazon.device.messaging.permission.RECEIVE	unknown	Unknown permission	Unknown permission from android reference
com.alinma.retail.mobile.permission.RECEIVE_ADM_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
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.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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
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	signature	C2DM permissions	Permission for cloud to device messaging.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	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.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
possible ro.secure check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.alinma.retail.mobile.MainActivity	Schemes: alinmabanksmartphoneapp://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Application Data can be Backed up [android:allowBackup] flag is missing.	medium	The flag [android:allowBackup] should be set to false. By default it is set to true and allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Broadcast Receiver (nl.xservices.plugins.ShareChooserPendingIntent) is not Protected. An intent-filter exists.	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
4	Broadcast Receiver (com.pushwoosh.PushAmazonReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.amazon.device.messaging.permission.SEND [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
5	Broadcast Receiver (com.pushwoosh.BootReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.RECEIVE_BOOT_COMPLETED [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
6	Service (com.pushwoosh.FcmRegistrationService) is not Protected. An intent-filter exists.	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Service (com.pushwoosh.PushFcmIntentService) is not Protected. An intent-filter exists.	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.
8	Content Provider (com.pushwoosh.PushwooshSharedDataProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	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]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
10	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
11	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]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/pushwoosh/internal/preference/PreferenceVibrateTypeValue.java com/pushwoosh/notification/builder/a.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/pushwoosh/internal/utils/g.java com/pushwoosh/inapp/view/a/d.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/Engine.java com/pushwoosh/q.java com/pushwoosh/internal/preference/PreferenceBooleanValue.java com/pushwoosh/internal/registrar/a.java com/pushwoosh/inapp/view/b/d.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/pushwoosh/BootReceiver.java com/cordova/plugin/android/fingerprintauth/FingerprintAuth.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/pushwoosh/inapp/c.java com/pushwoosh/inapp/e/a/c.java com/scottyab/rootbeer/RootBeer.java com/pushwoosh/HandleMessageWorker.java com/pushwoosh/internal/preference/PreferenceClassValue.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/pushwoosh/internal/utils/e.java com/pushwoosh/plugin/geolocation/LocationSettingsResolutionActivity.java com/pushwoosh/inapp/view/a.java com/pushwoosh/inbox/internal/a/c.java com/pushwoosh/inapp/e/c.java com/pushwoosh/internal/network/NetworkModule.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/pushwoosh/notification/handlers/message/user/d.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/pushwoosh/s.java com/pushwoosh/inbox/internal/data/InboxMessageStatus.java com/pushwoosh/internal/preference/PreferenceStringValue.java com/pushwoosh/inapp/view/RichMediaWebActivity.java com/pushwoosh/inapp/c/a.java com/pushwoosh/internal/utils/JsonUtils.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/pushwoosh/inbox/internal/data/b.java com/pushwoosh/internal/platform/prefs/a.java com/pushwoosh/inapp/c/b.java com/pushwoosh/secure/a/e.java com/cordova/plugin/android/fingerprintauth/FingerprintAuthenticationDialogFragment.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/pushwoosh/repository/RepositoryModule.java com/bumptech/glide/load/data/LocalUriFetcher.java com/pushwoosh/a.java com/pushwoosh/notification/LocalNotificationReceiver.java com/pushwoosh/repository/PushBundleStorageImpl.java com/pushwoosh/secure/c/a/d.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/pushwoosh/secure/crypt/c/a/d.java com/pushwoosh/inapp/view/b/f.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/lampa/startapp/startApp.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 (high) CWE: CWE-532 Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/bumptech/glide/manager/RequestManagerRetriever.java com/scottyab/rootbeer/util/QLog.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/load/engine/DecodePath.java com/pushwoosh/richmedia/a.java com/pushwoosh/j.java com/pushwoosh/plugin/PushwooshSecure.java com/pushwoosh/internal/platform/prefs/migration/MigrationScheme.java com/quiply/cordova/saveimage/SaveImage.java com/pushwoosh/thirdpart/com/ironz/binaryprefs/dump/DumpReceiver.java com/pushwoosh/internal/command/CommandApplayer.java com/bumptech/glide/Glide.java com/bumptech/glide/util/pool/FactoryPools.java com/alinma/tls/TlsCheckerPlugin.java com/pushwoosh/inbox/internal/data/InboxMessageSource.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/pushwoosh/richmedia/RichMedia.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/pushwoosh/inbox/data/InboxMessageType.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/pushwoosh/inbox/d/v.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/pushwoosh/notification/a.java com/pushwoosh/notification/builder/NotificationBuilderManager.java com/pushwoosh/secure/crypt/manager/a/a.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/pushwoosh/inapp/a.java com/pushwoosh/inbox/d/t.java com/pushwoosh/secure/crypt/c/b/a.java com/bumptech/glide/load/engine/SourceGenerator.java com/pushwoosh/notification/NotificationServiceExtension.java com/pushwoosh/repository/t.java com/pushwoosh/notification/b.java com/scottyab/aescrypt/AESCrypt.java com/pushwoosh/internal/utils/PWLog.java com/pushwoosh/internal/platform/utils/GeneralUtils.java com/pushwoosh/inbox/internal/a/a.java com/pushwoosh/internal/checker/b.i

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ava com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/pushwoosh/secure/crypt/a/b.java com/pushwoosh/repository/ab.java com/pushwoosh/inapp/a/a.java com/pushwoosh/internal/network/f.java com/bumptech/glide/load/model/ResourceLoader.java com/pushwoosh/internal/preference/PreferenceArrayListValue.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/pushwoosh/internal/platform/utils/a.java com/pushwoosh/inapp/view/a/b.java com/pushwoosh/notification/RescheduleNotificationsWorker.java com/pushwoosh/internal/preference/PreferenceJsonObjectValue.java com/pushwoosh/inapp/f/b.java com/pushwoosh/NotificationOpenReceiver.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/pushwoosh/inapp/view/b/g.java com/pushwoosh/inbox/internal/a/g.java com/pushwoosh/secure/crypt/manager/a.java com/pushwoosh/notification/e.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/pushwoosh/inapp/view/b/h.java com/pushwoosh/PushwooshWorkManagerHelper.java com/lampa/startapp/Assets.java com/pushwoosh/internal/utils/LockScreenReceiver.java com/pushwoosh/internal/preference/PreferenceSoundTypeValue.java com/pushwoosh/inbox/e/b/b.java com/andreszs/smsretriever/SMSRetriever.java com/pushwoosh/internal/preference/PreferenceLongValue.java com/pushwoosh/repository/LockScreenMediaStorageImpl.java com/pushwoosh/repository/c.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/pushwoosh/PushAmazonIntentService.java com/pushwoosh/secure/crypt/c/e/c.java com/pushwoosh/inapp/view/b/a/b.java com/pushwoosh/notification/Action.j

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/pushwoosh/notification/NotificationActivity.java com/pushwoosh/secure/PushwooshSecure.java com/phonegap/plugins/barcodescanner/BarcodeScanner.java com/pushwoosh/notification/handlers/notification/b.java com/pushwoosh/internal/crash/a.java com/pushwoosh/badge/d/a/c.java com/pushwoosh/plugin/pushnotifications/PushNotifications.java com/bumptech/glide/request/SingleRequest.java com/pushwoosh/repository/InboxNotificationStorageImpl.java com/pddstudio/preferences/encrypted/EncryptedPreferences.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/pushwoosh/repository/n.java com/scottyab/rootbeer/RootBeerNative.java com/pushwoosh/plugin/PushGeolocation.java com/bumptech/glide/util/ContentLengthInputStream.java com/pushwoosh/amazon/a/a/a.java com/pushwoosh/internal/utils/PermissionActivity.java com/bumptech/glide/load/data/AssetPathFetcher.java com/pushwoosh/m.java com/pushwoosh/internal/platform/a/b.java com/pushwoosh/secure/crypt/c/e/a/b.java com/bumptech/glide/manager/RequestTracker.java com/pushwoosh/internal/preference/PreferenceIntValue.java com/bumptech/glide/load/engine/GlideException.java com/pushwoosh/DeepLinkActivity.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/pushwoosh/notification/SummaryNotificationFactory.java com/pushwoosh/internal/utils/NotificationRegistrarHelper.java com/pushwoosh/plugin/pushnotifications/PushwooshNotificationServiceExtension.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/pushwoosh/PushwooshFcmHelper.java com/pushwoosh/inapp/view/i.java com/pushwoosh/secure/crypt/manager/RsaDecryptorManager.java com/pushwoosh/secure/crypt/c/d/c.java com/pushwoosh/notification/SummaryNotificationUtils.java com/pushwoosh/internal/network/e

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/pushwoosh/internal/network/e.java com/pushwoosh/repository/d.java com/pushwoosh/repository/i.java com/pushwoosh/GDPRManager.java com/bumptech/glide/request/target/ViewTarget.java com/pushwoosh/inapp/a/k.java com/bumptech/glide/load/model/FileLoader.java com/pushwoosh/secure/crypt/c/e/d.java com/pushwoosh/internal/registrar/RegistrarWorker.java
2	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CVSS V2: 7.4 (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	com/cordova/plugin/android/fingerprintauth/FingerprintAuth.java com/pushwoosh/secure/a/a.java com/pushwoosh/internal/a/a.java
3	App can read/write to External Storage. Any App can read data written to External Storage.	high	CVSS V2: 5.5 (medium) CWE: CWE-276 Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/darktalker/cordova/screenshot/Screenshot.java com/quiply/cordova/saveimage/SaveImage.java com/pushwoosh/internal/platform/utils/a.java nl/xservices/plugins/SocialSharing.java
4	This App may have root detection capabilities.	secure	CVSS V2: 0 (info) OWASP MASVS: MSTG-RESILIENCE-1	com/scottyab/rootbeer/RootBeer.java com/pushwoosh/internal/platform/utils/a.java de/cyberkatze/iroot/IRoot.java
5	MD5 is a weak hash known to have hash collisions.	warning	CVSS V2: 7.4 (high) CWE: CWE-327 Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/pushwoosh/internal/utils/e.java com/pushwoosh/internal/platform/utils/GeneralUtils.java
6	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CVSS V2: 7.4 (high) CWE: CWE-312 Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/bumptech/glide/load/engine/ResourceCacheKey.java com/pushwoosh/plugin/geolocation/LocationPushesStorage.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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	CVSS V2: 5.9 (medium) CWE: CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/pushwoosh/repository/PushBundleStorageImpl.java com/pushwoosh/internal/network/f.java com/pushwoosh/inapp/f/b.java com/pushwoosh/inbox/e/b/b.java com/pushwoosh/repository/LockScreenMediaStorageImpl.java com/pushwoosh/repository/c.java com/pushwoosh/repository/InboxNotificationStorageImpl.java
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	CVSS V2: 0 (info) OWASP MASVS: MSTG-NETWORK-4	com/pushwoosh/secure/crypt/manager/a/a.java
9	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	CVSS V2: 0 (info) OWASP MASVS: MSTG-STORAGE-10	nl/xservices/plugins/SocialSharing.java com/verso/cordova/clipboard/Clipboard.java
10	This App may request root (Super User) privileges.	high	CVSS V2: 0 (info) CWE: CWE-250 Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/scottyab/rootbeer/Const.java
11	The App uses an insecure Random Number Generator.	warning	CVSS V2: 7.5 (high) CWE: CWE-330 Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/pushwoosh/internal/a/d.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/x86/libtool-checker.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.
2	lib/x86_64/libtool-checker.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/armeabi-v7a/libtool-checker.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/arm64-v8a/libtool-checker.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	False info The shared object does not have run-time search path or RPATH set.	False info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['location', 'network connectivity', 'camera'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.
12	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit.
13	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
14	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
15	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
16	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
17	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
18	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
s.api.pushwoosh.com	good	**IP:** 88.198.209.122 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
api.whatsapp.com	good	**IP:** 157.240.196.60 **Country:** France **Region:** Provence-Alpes-Cote-d'Azur **City:** Marseille **Latitude:** 43.296951 **Longitude:** 5.381070 **View:** Google Map
pddstudio.com	good	**IP:** 46.30.215.43 **Country:** Denmark **Region:** Hovedstaden **City:** Copenhagen **Latitude:** 55.675941 **Longitude:** 12.565530 **View:** Google Map
github.com	good	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
goo.gl	good	**IP:** 142.250.186.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
go.pushwoosh.com	good	**IP:** 88.198.239.122 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
cp.pushwoosh.com	good	**IP:** 88.198.239.120 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
sdk.hockeyapp.net	good	**IP:** 40.70.164.17 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map

URLS

URL	FILE
javascript:handleOpenURL('	de/martinreinhardt/cordova/plugins/urlhandler/LaunchMyApp.java
data:image	com/bumptech/glide/load/model/DataUrlLoader.java
file:///android_asset/	com/bumptech/glide/load/model/AssetUriLoader.java
	com/darktalker/cordova/screenshot/Screenshot.java
javascript:pwInlineInappSizeDelegate.resize(document.body.clientWidth,	com/pushwoosh/inapp/view/inline/e.java
javascript:_pwCallbackHelper.invokeCallback(javascript:(function	com/pushwoosh/inapp/view/a/d.java
javascript:%s(); javascript:%s('%s');	com/pushwoosh/inapp/view/a/b.java
https://%s.api.pushwoosh.com/json/1.3/ https://cp.pushwoosh.com/json/1.3/	com/pushwoosh/repository/RegistrationPrefs.java
https://go.pushwoosh.com/content/%s	com/pushwoosh/notification/handlers/notification/a.java
https://goo.gl/UVJKfp	com/pushwoosh/internal/checker/b.java

URL	FILE
https://sdk.hockeyapp.net/	com/pushwoosh/internal/crash/j.java
data:image/ https://api.whatsapp.com/send?phone=	nl/xservices/plugins/SocialSharing.java
http://pddstudio.com/ https://github.com/PDDStudio/EncryptedPreferences	Android String Resource

EMAILS

EMAIL	FILE
someone@domain.com	nl/xservices/plugins/SocialSharing.java

TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Pushwoosh		https://reports.exodus-privacy.eu.org/trackers/39

HARDCODED SECRETS

POSSIBLE SECRETS
"fingerprint_auth_dialog_title" : "Fingerprint Authentication"
"library_EncryptedPreferences_author" : "Patrick J"
"library_EncryptedPreferences_authorWebsite" : "http://pddstudio.com/"
"fingerprint_auth_dialog_title" : "Autenticación de Huellas Digitales"

App Security Score Calculation

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

Risk Calculation

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

Report Generated by - MobSF v3.4.5 Beta

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