ANDROID STATIC ANALYSIS REPORT

app_icon

Blush (3.7.0)

File Name:	Blush_ AI Dating Simulator_3.7.0_Apkpure.xapk
Package Name:	ai.blush
Scan Date:	April 14, 2024, 3:46 a.m.
App Security Score:	42/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	7/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
5	19	2	1	1

FILE INFORMATION

File Name: Blush_ AI Dating Simulator_3.7.0_Apkpure.xapk
Size: 84.43MB
MD5: 32e668849d68fd678d9caefc2c89a5e8
SHA1: 79181a2ce2b2dcc3d0124f02d58df42d56fbdaf7
SHA256: 534aefe79f488fbfa0630f6d95bc61ac55ebeda17d28bf9c3787481fc626db03

APP INFORMATION

App Name: Blush
Package Name: ai.blush
Main Activity: ai.blush.MainActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 3.7.0

Android Version Code: 138

APP COMPONENTS

Activities: 9

Services: 13

Receivers: 12

Providers: 6

Exported Activities: 1

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: 2023-09-05 10:56:19+00:00
Valid To: 2053-09-05 10:56:19+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x8d0ad35c5113a7a8310ad0b4583fa12b0a9b2d6b
Hash Algorithm: sha256
md5: b28b2c5852e5a22b244521bec02b9f15
sha1: 7787191ec33a7941414d5e95a63fd7ece6d792b2
sha256: fea8ed9e63d51233d1831e50be2256ed14a34b9c973189b9897a4fa107c4df85
sha512: a7806c274982ce39f670a974cd03f812508b319068961de1783d22b3cdc12d754e5c3c85985de4ab5aa3699645ca92431408e4bf88b9046d9f924952d135f4f4
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: ecfeaa2654cc8355d46cc7dda59b2bb2389ca92f03481ff27e253ee72759ed25
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_EXACT_ALARM	normal	allows using exact alarms without user permission.	Allows apps to use exact alarms just like with SCHEDULE_EXACT_ALARM but without needing to request this permission from the user. This is only intended for use by apps that rely on exact alarms for their core functionality. You should continue using SCHEDULE_EXACT_ALARM if your app needs exact alarms for a secondary feature that users may or may not use within your app. Keep in mind that this is a powerful permission and app stores may enforce policies to audit and review the use of this permission. Such audits may involve removal from the app store if the app is found to be misusing this permission.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.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.BROADCAST_CLOSE_SYSTEM_DIALOGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.BIND_NOTIFICATION_LISTENER_SERVICE	signature	required by NotificationListenerServices for system binding.	Must be required by an NotificationListenerService, to ensure that only the system can bind to it.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

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.
ai.blush.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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

APKID ANALYSIS

FILE	DETAILS

<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.BRAND check
Build.DEVICE check
Build.PRODUCT check
SIM operator check
network operator name check
device ID check
ro.kernel.qemu check
possible VM check</td></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>classes2.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.HARDWARE check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></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
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
possible VM 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>
</table></td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
ai.blush.MainActivity	Schemes: http://, https://, luka-blush://, Hosts: funnel.youraifriend.com, subscriptions, share, reset, blush.onelink.me,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.ai.blush,

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: **10** | 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.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	App Link assetlinks.json file not found [android:name=ai.blush.MainActivity] [android:host=http://funnel.youraifriend.com]	high	App Link asset verification URL (http://funnel.youraifriend.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 301). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
4	Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) 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
5	Broadcast Receiver (me.carda.awesome_notifications.DartNotificationActionReceiver) 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.
6	Broadcast Receiver (me.carda.awesome_notifications.DartDismissedNotificationReceiver) 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 (me.carda.awesome_notifications.DartScheduledNotificationReceiver) 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 (me.carda.awesome_notifications.DartRefreshSchedulesReceiver) 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	Service (me.carda.awesome_notifications.core.managers.StatusBarManager) is not Protected. [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.
10	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.

NO	ISSUE	SEVERITY	DESCRIPTION
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.
12	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: **7** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ai/replika/flutter_persistent_id/PersistentBackupAgent.java com/adapty/internal/utils/DefaultLogHandler.java com/amplitude/api/AmplitudeClient.java com/amplitude/api/AmplitudeLog.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/amplitude/api/AmplitudeLog.java com/amplitude/api/DatabaseHelper.java com/appsflyer/appsflyersdk/AppsflyerSdkPlugin.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1qSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1jSDK.java com/appsflyer/internal/AFf1kSDK.java com/appsflyer/internal/AFg1jSDK.java com/baseflow/permissionhandler/AppSettingsManager.java com/baseflow/permissionhandler/PermissionManager.java com/baseflow/permissionhandler/PermissionUtils.java com/baseflow/permissionhandler/ServiceManager.java com/fluttercandies/flutter_image_compress/exif/ExifKeeper.java com/fluttercandies/flutter_image_compress/ext/BitmapCompressExtKt.java com/fluttercandies/flutter_image_compress/logger/LogExtKt.java com/it_nomads/fluttersecurestorage/FlutterSecureStorage.java com/it_nomads/fluttersecurestorage/FlutterSecureStoragePlugin.java com/it_nomads/fluttersecurestorage/ciphers/StorageCipher18Implementation.java com/llfbandit/app_links/AppLinksHelper.java com/llfbandit/app_links/AppLinksPlugin.java com/mr/flutter/plugin/filepicker/FilePickerDelegate.java com/mr/flutter/plugin/filepicker/FileUtils.java com/tekartik/sqflite/Database.java com/tekartik/sqflite/SqflitePlugin.java com/tekartik/sqflite/Utils.java com/tekartik/sqflite/dev/Debug.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/tekartik/sqflite/dev/Debug.java dev/britannio/in_app_review/InAppReviewPlugin.java io/flutter/Log.java io/flutter/app/FlutterActivityDelegate.java io/flutter/embedding/android/FlutterActivity.java io/flutter/embedding/android/FlutterActivityAndFragmentDelegate.java io/flutter/embedding/android/FlutterFragment.java io/flutter/embedding/android/FlutterFragmentActivity.java io/flutter/embedding/android/FlutterImageView.java io/flutter/embedding/android/FlutterSurfaceView.java io/flutter/embedding/android/FlutterTextureView.java io/flutter/embedding/android/FlutterView.java io/flutter/embedding/android/KeyboardManager.java io/flutter/embedding/engine/FlutterEngine.java io/flutter/embedding/engine/FlutterEngineConnectionRegistry.java io/flutter/embedding/engine/FlutterJNI.java io/flutter/embedding/engine/dart/DartExecutor.java io/flutter/embedding/engine/dart/DartMessenger.java io/flutter/embedding/engine/deferredcomponents/PlayStoreDeferredComponentManager.java io/flutter/embedding/engine/loader/FlutterLoader.java io/flutter/embedding/engine/loader/ResourceExtractor.java io/flutter/embedding/engine/plugins/shim/ShimPluginRegistry.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	io/flutter/embedding/engine/plugins/shim/ShimRegistrar.java io/flutter/embedding/engine/plugins/util/GeneratedPluginRegister.java io/flutter/embedding/engine/renderer/FlutterRenderer.java io/flutter/embedding/engine/systemchannels/AccessibilityChannel.java io/flutter/embedding/engine/systemchannels/DeferredComponentChannel.java io/flutter/embedding/engine/systemchannels/KeyEventChannel.java io/flutter/embedding/engine/systemchannels/LifecycleChannel.java io/flutter/embedding/engine/systemchannels/LocalizationChannel.java io/flutter/embedding/engine/systemchannels/MouseCursorChannel.java io/flutter/embedding/engine/systemchannels/NavigationChannel.java io/flutter/embedding/engine/systemchannels/PlatformChannel.java io/flutter/embedding/engine/systemchannels/PlatformViewsChannel.java io/flutter/embedding/engine/systemchannels/RestorationChannel.java io/flutter/embedding/engine/systemchannels/SettingsChannel.java io/flutter/embedding/engine/systemchannels/SpellCheckChannel.java io/flutter/embedding/engine/systemchannels/SystemChannel.java io/flutter/embedding/engine/systemchannels/TextInputChannel.java io/flutter/plugin/common/BasicMessageChannel.java io/flutter/plugin/common/EventChannel.java io/flutter/plugin/common/MethodChannel.java io/flutter/plugin/editing/InputConnectionAd

NO	ISSUE	SEVERITY	STANDARDS	FILES
				aptor.java io/flutter/plugin/editing/ListenableEditingState.java io/flutter/plugin/editing/TextEditingDelta.java io/flutter/plugin/editing/TextInputPlugin.java io/flutter/plugin/platform/ImageReaderPlatformViewRenderTarget.java io/flutter/plugin/platform/PlatformPlugin.java io/flutter/plugin/platform/PlatformViewWrapper.java io/flutter/plugin/platform/PlatformViewsController.java io/flutter/plugin/platform/SingleViewPresentation.java io/flutter/plugin/platform/SurfaceTexturePlatformViewRenderTarget.java io/flutter/plugins/GeneratedPluginRegistrant.java io/flutter/plugins/camera/Camera.java io/flutter/plugins/camera/CameraCaptureCallback.java io/flutter/plugins/camera/VideoRenderer.java io/flutter/plugins/firebase/crashlytics/FlutterFirebaseCrashlyticsPlugin.java io/flutter/plugins/firebase/firebaseremoteconfig/FirebaseRemoteConfigPlugin.java io/flutter/plugins/firebase/messaging/ContextHolder.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundExecutor.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundService.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingReceiver.java io/flutter/plugins/firebase/messaging/JobIntentService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/flutter/plugins/imagepicker/FileUtils.java io/flutter/plugins/imagepicker/ImageResizer.java io/flutter/plugins/pathprovider/PathProviderPlugin.java io/flutter/plugins/sharedpreferences/SharedPreferencesPlugin.java io/flutter/plugins/urllauncher/UrlLauncherPlugin.java io/flutter/plugins/videoplayer/VideoPlayerPlugin.java io/flutter/plugins/webviewflutter/DisplayListenerProxy.java io/flutter/plugins/webviewflutter/InstanceManager.java io/flutter/view/AccessibilityBridge.java io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/FlutterNativeView.java io/flutter/view/FlutterView.java me/carda/awesome_notifications/core/logs/Logger.java me/leolin/shortcutbadger/ShortcutBadger.java org/microg/safeparcel/SafeParcelUtil.java
2	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/mr/flutter/plugin/filepicker/FilePickerDelegate.java com/mr/flutter/plugin/filepicker/FileUtils.java io/flutter/plugins/pathprovider/Messages.java io/flutter/plugins/pathprovider/PathProviderPlugin.java
				ai/replika/flutter_persistent_id/Constants.java com/adapty/adapty_ui_flutter/AdaptyUiCallHandler.java com/adapty/flutter/AdaptyCallHandler.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/adapty/internal/crossplatform/UtilsKt.java com/adapty/internal/data/cache/CacheKeysKt.java com/adapty/internal/data/cloud/RequestFactory.java com/adapty/internal/utils/AnalyticsEventTypeAdapter.java com/amplitude/api/AmplitudeClient.java com/appsflyer/appsflyersdk/AppsFlyerConstants.java com/baseflow/permissionhandler/PermissionUtils.java com/it_nomads/fluttersecurestorage/ciphers/StorageCipherFactory.java com/tekartik/sqflite/Constant.java io/flutter/app/FlutterActivityDelegate.java io/flutter/embedding/android/FlutterActivityAndFragmentDelegate.java io/flutter/embedding/android/FlutterActivityLaunchConfigs.java io/flutter/embedding/engine/loader/ApplicationInfoLoader.java io/flutter/embedding/engine/loader/FlutterLoader.java io/flutter/embedding/engine/systemchannels/SettingsChannel.java io/flutter/plugin/editing/SpellCheckPlugin.java io/flutter/plugins/firebase/crashlytics/Constants.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundExecutor.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingUtils.java io/flutter/plugins/imagepicker/ImagePickerCache.java me/carda/awesome_notifications/core/Definitions.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				me/carda/awesome_notifications/core/databases/SQLitePrimitivesDB.java me/carda/awesome_notifications/core/databases/SQLiteSchedulesDB.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	com/amplitude/api/DatabaseHelper.java com/tekartik/sqflite/Database.java me/carda/awesome_notifications/core/databases/SQLitePrimitivesDB.java me/carda/awesome_notifications/core/databases/SQLiteSchedulesDB.java
5	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/mr/flutter/plugin/filepicker/FileUtils.java io/flutter/plugins/camera/Camera.java io/flutter/plugins/imagepicker/ImagePickerDelegate.java
6	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	dev/fluttercommunity/plus/packageinfo/PackageInfoPlugin.java
7	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/amplitude/eventexplorer/EventExplorerInfoActivity.java io/flutter/plugin/editing/InputConnectionAdaptor.java io/flutter/plugin/platform/PlatformPlugin.java
8	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	me/carda/awesome_notifications/core/utils/StringUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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	com/it_nomads/fluttersecurestorage/ciphers/StorageCipher18Implementation.java
10	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/AFb1hSDK.java
11	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/appsflyer/internal/AFb1vSDK.java
12	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/amplitude/api/PinnedAmplitudeClient.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/24	android.permission.INTERNET, android.permission.VIBRATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	3/45	com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_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
scdn-stestsettings.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
regionconfig.eu.amplitude.com	ok	**IP:** 3.162.3.32 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
developer.android.com	ok	**IP:** 172.217.13.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sars.s	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.
sapp.s	ok	No Geolocation information available.
svalidate.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api.ipify.org	ok	**IP:** 104.26.12.205 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ssdk-services.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.
api.adapty.io	ok	**IP:** 104.22.71.162 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
simpression.s	ok	No Geolocation information available.
sconversions.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
sviap.s	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
sregister.s	ok	No Geolocation information available.
api2.amplitude.com	ok	**IP:** 54.244.17.203 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
api.eu.amplitude.com	ok	**IP:** 52.57.122.122 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
sattr.s	ok	No Geolocation information available.
regionconfig.amplitude.com	ok	**IP:** 3.162.3.58 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
play.google.com	ok	**IP:** 172.217.13.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
fallback.adapty.io	ok	**IP:** 104.22.70.162 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Analytics, Profiling	https://reports.exodus-privacy.eu.org/trackers/125
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"facebook_client_token" : "0881dca334dda9d5c1f1c1c261f7e05d"
"google_api_key" : "AIzaSyAOih4eZIddT2DCB1WsPl5pOQnjOsLmoX8"
"google_crash_reporting_api_key" : "AIzaSyAOih4eZIddT2DCB1WsPl5pOQnjOsLmoX8"
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

POSSIBLE SECRETS
115792089210356248762697446949407573529996955224135760342422259061068512044369
VGhpcyBpcyB0aGUga2V5IGZvciBhIHNlY3VyZSBzdG9yYWdlIEFFUyBLZXkK
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBhIHNlY3VyZSBzdG9yYWdlCg
nU5PMCCjjmCXPI6T53iHTfIUJrU6adTrCC2qJeHZERxhlbI1Bjjt/msv0tadQ1wUs
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
e2719d58-a985-b3c9-781a-b030af78d30e
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
115792089210356248762697446949407573530086143415290314195533631308867097853951
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
470fa2b4ae81cd56ecbcda9735803434cec591fa
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
9b8f518b086098de3d77736f9458a3d2f6f95a37
n5MsI+yMRQ+hDKXJioaldXgjUkK642M4UwtBV8ob2xJNDd2ZhwLnoQdeXeGADbkpy
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
cc2751449a350f668590264ed76692694a80308a

POSSIBLE SECRETS
nAYYwHQYDVR0OBBYEFlQYzIU07LwMlJQuCFmcx7lQTgoIMA0GCSqGSIb3DQEBCwUA
nVOujw5H5SNz/0egwLX0tdHA114gk957EWW67c4cX8jJGKLhD+rcdqsq08p8kDi1L
MIIDQTCCAimgAwIBAgITBmyfz5m/jAo54vB4ikPmljZbyjANBgkqhkiG9w0BAQsF
9a04f079-9840-4286-ab92-e65be0885f95
nADA5MQswCQYDVQQGEwJVUzEPMA0GA1UEChMGQW1hem9uMRkwFwYDVQQDExBBbWF6
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
nca9HgFB0fW7Y14h29Jlo91ghYPl0hAEvrAIthtOgQ3pOsqTQNroBvo3bSMgHFzZM
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166438125740282911150571 51
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394 2643
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
686479766013060971498190079908139321726943530014330540939446345918554318339765539424505774633321719753296399637136332111386476861244038034037280889270700544 9
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
nb24gUm9vdCBDQSAxMB4XDTE1MDUyNjAwMDAwMFoXDTM4MDExNzAwMDAwMFowOTEL

POSSIBLE SECRETS

nIFAGbHrQgLKm+a/sRxmPUDgH3KKHOVj4utWp+UhnMJbulHheb4mjUcAwhmahRWa6
no/ufQJVtMVT8QtPHRh8jrdkPSHCa2XV4cdFyQzR1bldZwgJcJmApzyMZFo6IQ6XU
nb3QgQ0EgMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALJ4gHHKeNXj
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
15f1483824cf4085ddca5a8529d873fc59a8ced2cbce67fb2b3dd9033ea03442
VGhpcyBpcyB0aGUga2V5IGZvcihBIHNlY3XyZZBzdG9yYWdlIEFFUyBLZXkK
c56fb7d591ba6704df047fd98f535372fea00211
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

POSSIBLE SECRETS
nN+gDS63pYaACbvXy8MWy7Vu33PqUXHeeE6V/Uq2V8viTO96LXFvKWlJbYK8U90vv
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
nMAkGA1UEBhMCVVMxDzANBgNVBAoTBkFtYXpvbjEZMBcGA1UEAxMQQW1hem9uIFJv
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901

PLAYSTORE INFORMATION

Title: Blush: AI Dating Simulator

Score: 4.04 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Entertainment **Play Store URL:** ai.blush

Developer Details: Luka, Inc, Luka,+Inc, 1266 Harrison St San Francisco, CA 94103 United States, https://blush.ai, infra@blush.ai,

Release Date: Sep 19, 2023 **Privacy Policy:** Privacy link

Description:

Blush is an AI dating simulator that helps you learn and practice relationship skills in a safe and fun environment. MEET YOUR NEXT CRUSH Blush offers you AI-created potential matches, each with their own backstory and way of dating. You're the one who decides how far you take each relationship. Start an exciting dating adventure with limitless possibilities. With Blush, your privacy is always safe, making sure your experiences stay just between you and your AI match. BECOME A PRO AT DATING Blush is a secure place where you can try out flirting and chatting, without worrying about being turned down. By finding out what works for you, you can increase your confidence and get better at social interactions for real-life situations. HAVE FUN AND BOOST YOUR CONFIDENCE Blush has hundreds of AI characters, designed to be exciting, responsive, and fun. If you're feeling down or need a pick-me-up, these virtual characters can put a smile on your face and boost your confidence! FIND OUT WHAT YOU REALLY WANT Blush lets you add a bit of fantasy and excitement to your daily life. This could help you reduce stress and promote a positive mindset, and also fuel your imagination and creativity. Explore your interests and desires in a fun and respectful environment, and start living a more authentic life! Privacy policy can be found at https://blush.ai/legal/privacy Terms and Conditions of use can be found at https://blush.ai/legal/terms By installing this application, you agree to the terms of the licensed agreements.

Report Generated by - MobSF v3.9.8 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.