



ANDROID STATIC ANALYSIS REPORT



 iAccess Life (1.2.0)

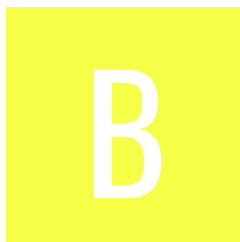
File Name: iAccess Life - Accessibility_1.2.0_APKPure.apk

Package Name: com.iaccessapp

Scan Date: Nov. 27, 2024, 1:20 a.m.






App Security Score: 46/100 (MEDIUM RISK)

Grade:



Trackers Detection: 8/432

FINDINGS SEVERITY

|  HIGH |  MEDIUM |  INFO |  SECURE |  HOTSPOT |
|--|--|--|--|---|
| 4 | 12 | 3 | 2 | 1 |

FILE INFORMATION

File Name: iAccess Life - Accessibility_1.2.0_APKPure.apk

Size: 19.66MB

MD5: 8632b7f471a29a9c1be8b3334ea395e2

SHA1: 065f327bd3ff75a6d3f87d6fc6867592f1a9b022

SHA256: ba9adfb92ef1190e173dc17489d87dfe37accf5c39669ee4d764f6e1db6d5cd8

APP INFORMATION

App Name: iAccess Life

Package Name: com.iaccessapp

Main Activity: com.iaccess.activity.SplashActivity

Target SDK: 28

Min SDK: 21

Max SDK:

Android Version Name: 1.2.0

Android Version Code: 3

APP COMPONENTS

Activities: 32

Services: 8

Receivers: 5

Providers: 5

Exported Activities: 1

Exported Services: 2

Exported Receivers: 2

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: 2019-03-14 09:13:09+00:00

Valid To: 2049-03-14 09:13:09+00:00

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

Serial Number: 0x7d55f7a68d3e33298e7cb71b7ba1fe43aba21ea

Hash Algorithm: sha256

md5: 77da0d844d6b517fd47a8a335e15bcf2

sha1: f4f504c8d786c9763a211c5678c420f6ff3d885b

sha256: 5970fb8ac6886e23a85daff38c62c5c7b0900c44c77ad2962e1c37ee9e07c637

sha512: 2005db76f70f523229865908d078464a13be4e560d7e1f3d7c009ca431bc22e43d5fa9fe71b042ffaa1334f091a004e2720769c82af0db0f88e974cc5b29d7ab

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 94db1d2ab33bcf453ec7f5937d5f70465b9f5dec5d04401cc1979e1dceb2c6ff

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.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.GET_ACCOUNTS | dangerous | list accounts | Allows access to the list of accounts in the Accounts Service. |
| android.permission.ACCESS_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. |
| 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.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. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|--|-----------|---------------------------------|---|
| android.permission.ACCESS_COARSE_LOCATION | dangerous | coarse (network-based) location | Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are. |
| com.example.permission.MAPS_RECEIVE | unknown | Unknown permission | Unknown permission from android reference |
| com.iaccessapp.provider.READ | 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 | normal | recieve push notifications | Allows an application to receive push notifications from cloud. |
| com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE | normal | permission defined by google | A custom permission defined by Google. |

APKID ANALYSIS

| FILE | DETAILS |
|------|---------|
|------|---------|

| FILE | DETAILS | |
|--------------|-----------------|---|
| classes.dex | FINDINGS | DETAILS |
| | Anti-VM Code | Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible VM check |
| | Compiler | r8 |
| classes2.dex | FINDINGS | DETAILS |
| | Anti-VM Code | Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check network operator name check possible VM check |
| | Anti Debug Code | Debug.isDebuggerConnected() check |
| | Compiler | r8 without marker (suspicious) |

| ACTIVITY | INTENT |
|-------------------------------------|---|
| com.facebook.CustomTabActivity | Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.com.iaccessapp, |
| com.iaccess.activity.SplashActivity | Schemes: iaccessapp://, https://, Hosts: open, 2s8w.test-app.link, |

NETWORK SECURITY

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

| NO | SCOPE | SEVERITY | DESCRIPTION |
|----|-------|----------|---|
| 1 | * | high | Base config is insecurely configured to permit clear text traffic to all domains. |

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: 5 | INFO: 0 | SUPPRESSED: 0

| NO | ISSUE | SEVERITY | DESCRIPTION |
|----|--|----------|--|
| 1 | App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21] | 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 | App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config] | info | The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app. |
| 3 | Activity (com.facebook.CustomTabActivity) is vulnerable to StrandHogg 2.0 | high | Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (28) of the app to 29 or higher to fix this issue at platform level. |
| 4 | 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 |
|----|--|----------|--|
| 5 | Service (com.iaccess.fcmservice.FCMMessagingService) is Protected by a permission, but the protection level of the permission should be checked. Permission: false [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. |
| 6 | Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true] | warning | A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission. |
| 7 | 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 |
|----|--|----------|---|
| 8 | <p>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]</p> | warning | <p>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.</p> |

</> CODE ANALYSIS

HIGH: 0 | WARNING: 5 | INFO: 2 | SECURE: 1 | SUPPRESSED: 0

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|-------|----------|-----------|--|
| | | | | <p>bolts/MeasurementEvent.java butterknife/ButterKnife.java com/beloo/widget/chipslayoutmanager/ChipsLayoutMa nager.java com/beloo/widget/chipslayoutmanager/cache/ViewCac heStorage.java com/beloo/widget/chipslayoutmanager/util/log/Androi dLog.java com/beloo/widget/chipslayoutmanager/util/log/FillLogg er.java com/bumptech/glide/Glide.java com/bumptech/glide/disklruCache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.ja va com/bumptech/glide/load/data/AssetPathFetcher.java</p> |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|-------|----------|-----------|--|
| | | | | com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetc her.java com/bumptech/glide/load/data/mediastore/Thumbnail StreamOpener.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/SourceGenerator.jav a com/bumptech/glide/load/engine/bitmap_recycle/LruAr rayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBi tmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCache Wrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCa lculator.java com/bumptech/glide/load/engine/executor/GlideExecut or.java com/bumptech/glide/load/engine/executor/RuntimeCo mpat.java com/bumptech/glide/load/engine/prefill/BitmapPreFillR unner.java com/bumptech/glide/load/model/ByteBufferEncoder.ja va com/bumptech/glide/load/model/ByteBufferFileLoader. java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/ImageDecoderReso urceDecoder.java com/bumptech/glide/load/resource/bitmap/BitmapEnc oder.java com/bumptech/glide/load/resource/bitmap/BitmapIma geDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultIma geHeaderParser.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 | com/bumptech/glide/load/resource/bitmap/Downsample.java com/bumptech/glide/load/resource/bitmap/DrawableTransformer.java com/bumptech/glide/load/resource/bitmap/BitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/iaccess/SocialLoginHelper/GoogleSignInHelper.java com/iaccess/activity/MapViewActivity.java com/iaccess/api/ApiManager.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|-------|----------|-----------|---|
| | | | | com/iaccess/custom_views/ButtonWithCustomFont.java com/iaccess/db/notifications/NotificationsController.java a com/iaccess/utls/GetCurrentLocation.java com/iaccess/utls/Helpers.java com/iaccess/utls/MarkerClusterRenderer.java com/mikelau/croperino/CropImage.java com/steelkiwi/cropiwa/CropIwaView.java com/steelkiwi/cropiwa/image/CropIwaBitmapManager.java com/steelkiwi/cropiwa/util/CropIwaLog.java com/steelkiwi/cropiwa/util/ImageHeaderParser.java com/steelkiwi/cropiwa/util/LoadBitmapCommand.java com/yalantis/ucrop/UCropActivity.java com/yalantis/ucrop/task/BitmapCropTask.java com/yalantis/ucrop/task/BitmapLoadTask.java com/yalantis/ucrop/util/BitmapLoadUtils.java com/yalantis/ucrop/util/EglUtils.java com/yalantis/ucrop/util/FileUtils.java com/yalantis/ucrop/util/ImageHeaderParser.java com/yalantis/ucrop/view/TransformImageView.java io/branch/referral/PrefHelper.java io/branch/referral/validators/IntegrationValidator.java io/realm/BaseRealm.java io/realm/DynamicRealm.java io/realm/Realm.java io/realm/RealmCache.java io/realm/RealmObject.java io/realm/RealmResults.java io/realm/internal/FinalizerRunnable.java io/realm/internal/OsRealmConfig.java io/realm/internal/RealmCore.java io/realm/internal/Util.java me/zhanghai/android/materialratingbar/ClipDrawableCompat.java me/zhanghai/android/materialratingbar/MaterialRatingBar.java org/jetbrains/anko/Logging.java timber/log/Timber.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|--|----------|---|---|
| 2 | 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 | bolts/MeasurementEvent.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.java com/iaccess/activity/ChangePasswordActivity.java com/iaccess/utils/Constants.java io/branch/indexing/ContentDiscoverer.java io/branch/indexing/ContentDiscoveryManifest.java io/branch/referral/Branch.java io/branch/referral/BranchPreinstall.java io/branch/referral/DeferredAppLinkDataHandler.java io/branch/referral/PrefHelper.java io/branch/referral/ServerRequest.java io/branch/referral/ServerRequestQueue.java io/branch/referral/UniversalResourceAnalyser.java io/branch/referral/validators/DeepLinkRoutingValidator.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java |
| 3 | 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/iaccess/utils/ImagePickerController.java com/mikelau/croperino/CropImage.java com/mikelau/croperino/Croperino.java com/mikelau/croperino/CroperinoFileUtil.java com/yalantis/ucrop/util/FileUtils.java |
| 4 | 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/iaccess/fragment/ProfileFragment.java io/branch/referral/ShareLinkManager.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|--|----------|---|--|
| 5 | 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/iaccess/fcmService/FCMMessageService.java q/rorbin/badgeview/BadgeAnimator.java |
| 6 | 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 | bolts/WebViewAppLinkResolver.java |
| 7 | This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel. | secure | OWASP MASVS: MSTG-NETWORK-4 | com/iaccess/api/ApiController.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/mikelau/croperino/CroperinoFileUtil.java |

SHARED LIBRARY BINARY ANALYSIS

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

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|------------------------|---|--|---|--|---|---|--|---|
| 1 | x86_64/librealm-jni.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>False high</p> <p>This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p> | <p>Full RELRO info</p> <p>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.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary 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. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|----------------------|---|--|---|--|---|---|--|---|
| 2 | mips/librealm-jni.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>False high</p> <p>This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p> | <p>Full RELRO info</p> <p>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.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary 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. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-----------------------------|---|--|---|--|---|---|--|---|
| 3 | armeabi-v7a/librealm-jni.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>False high</p> <p>This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p> | <p>Full RELRO info</p> <p>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.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary 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. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|---------------------------|---|--|---|--|---|---|--|---|
| 4 | arm64-v8a/librealm-jni.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>False high</p> <p>This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p> | <p>Full RELRO info</p> <p>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.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary 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. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|---------------------|---|--|---|--|---|---|--|---|
| 5 | x86/librealm-jni.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary 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.</p> | <p>Full RELRO info</p> <p>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.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary 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. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|------------------------|---|--|---|--|---|---|--|---|
| 6 | x86_64/librealm-jni.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>False high</p> <p>This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p> | <p>Full RELRO info</p> <p>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.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary 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. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|----------------------|---|--|---|--|---|---|--|---|
| 7 | mips/librealm-jni.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>False high</p> <p>This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p> | <p>Full RELRO info</p> <p>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.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary 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. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-----------------------------|---|--|---|--|---|---|--|---|
| 8 | armeabi-v7a/librealm-jni.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>False high</p> <p>This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p> | <p>Full RELRO info</p> <p>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.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary 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. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|---------------------------|---|--|---|--|---|---|--|---|
| 9 | arm64-v8a/librealm-jni.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>False high</p> <p>This binary 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. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p> | <p>Full RELRO info</p> <p>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.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary 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. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|---------------------|---|--|---|--|---|---|--|---|
| 10 | x86/librealm-jni.so | True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably. | True info This binary 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. | None info The binary does not have run-time search path or RPATH set. | None info The binary does not have RUNPATH set. | False warning The binary 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. This check is not applicable for Dart/Flutter libraries. | True info Symbols are stripped. |

NIAP ANALYSIS v1.3

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

BEHAVIOUR ANALYSIS

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|---|------------|--|
| 00063 | Implicit intent(view a web page, make a phone call, etc.) | control | bolts/AppLinkNavigation.java bolts/AppLinks.java bolts/MeasurementEvent.java com/iaccess/SocialLoginHelper/FbConnectHelper.java com/iaccess/activity/MapViewActivity.java com/iaccess/activity/SplashActivity.java com/iaccess/activity/VenueDetailActivity.java com/iaccess/adapter/UserFavouriteAdapter.java com/iaccess/adapter/VenueListingAdapter.java com/iaccess/utils/Helpers.java io/branch/referral/Branch.java io/branch/referral/BranchStrongMatchHelper.java io/branch/referral/validators/DeepLinkRoutingValidator.java org/jetbrains/anko/IntentsKt.java |
| 00091 | Retrieve data from broadcast | collection | com/iaccess/activity/ImageEditActivity.java com/iaccess/activity/MapViewActivity.java com/iaccess/activity/SearchPlacesActivity.java com/iaccess/activity/VenueDetailActivity.java com/iaccess/activity/VenueLisingActivity.java com/iaccess/activity/ViewAllReviewsActivity.java com/iaccess/activity/WebViewActivity.java com/mikelau/croperino/CropImage.java io/branch/referral/Branch.java |
| 00051 | Implicit intent(view a web page, make a phone call, etc.) via setData | control | bolts/AppLinkNavigation.java com/iaccess/utils/Helpers.java io/branch/referral/Branch.java org/jetbrains/anko/IntentsKt.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|---|---------------------|--|
| 00036 | Get resource file from res/raw directory | reflection | bolts/AppLinkNavigation.java bolts/MeasurementEvent.java com/iaccess/utils/Helpers.java io/branch/referral/Branch.java |
| 00022 | Open a file from given absolute path of the file | file | com/getkeepsafe/relinker/ReLinkerInstance.java com/iaccess/utils/ImagePickerController.java com/steelkiwi/cropiwa/image/CroplwaBitmapManager.java io/realm/RealmConfiguration.java io/realm/internal/OsSharedRealm.java io/realm/internal/Util.java |
| 00016 | Get location info of the device and put it to JSON object | location collection | com/iaccess/activity/MapViewActivity.java com/iaccess/activity/VenueDetailActivity.java com/iaccess/adapter/VenueListingAdapter.java |
| 00013 | Read file and put it into a stream | file | com/bumptech/glide/disklruCache/DiskLruCache.java com/bumptech/glide/load/model/FileLoader.java com/getkeepsafe/relinker/elf/ElfParser.java com/mikelau/croperino/CroperinoFileUtil.java com/yalantis/ucrop/util/FileUtils.java okio/Okio.java |
| 00192 | Get messages in the SMS inbox | sms | com/yalantis/ucrop/util/FileUtils.java |
| 00125 | Check if the given file path exist | file | com/iaccess/activity/ImageEditActivity.java com/iaccess/fragment/ProfileFragment.java |
| 00202 | Make a phone call | control | org/jetbrains/anko/IntentsKt.java |
| 00203 | Put a phone number into an intent | control | org/jetbrains/anko/IntentsKt.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|---|---------------------------------|--|
| 00123 | Save the response to JSON after connecting to the remote server | network command | bolts/WebViewAppLinkResolver.java io/branch/referral/BranchViewHandler.java |
| 00089 | Connect to a URL and receive input stream from the server | command network | bolts/WebViewAppLinkResolver.java com/bumptechnology/load/data/HttpUrlFetcher.java io/branch/referral/BranchViewHandler.java |
| 00030 | Connect to the remote server through the given URL | network | bolts/WebViewAppLinkResolver.java com/bumptechnology/load/data/HttpUrlFetcher.java io/branch/referral/BranchViewHandler.java |
| 00109 | Connect to a URL and get the response code | network command | bolts/WebViewAppLinkResolver.java com/bumptechnology/load/data/HttpUrlFetcher.java io/branch/referral/BranchViewHandler.java |
| 00094 | Connect to a URL and read data from it | command network | bolts/WebViewAppLinkResolver.java io/branch/referral/BranchViewHandler.java |
| 00108 | Read the input stream from given URL | network command | bolts/WebViewAppLinkResolver.java io/branch/referral/BranchViewHandler.java |
| 00077 | Read sensitive data(SMS, CALLLOG, etc) | collection sms calllog calendar | com/bumptechnology/load/data/mediastore/ThumbFetcher.java |
| 00132 | Query The ISO country code | telephony collection | com/iaccess/fragment/DashBoardFragment.java |
| 00115 | Get last known location of the device | collection location | com/iaccess/Utils/GetCurrentLocation.java |
| 00078 | Get the network operator name | collection telephony | io/branch/referral/SystemObserver.java |
| 00147 | Get the time of current location | collection location | com/iaccess/Utils/Helpers.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|---|---------------------|---|
| 00112 | Get the date of the calendar event | collection calendar | com/iaccess/utls/Helpers.java |
| 00096 | Connect to a URL and set request method | command network | io/branch/referral/BranchViewHandler.java |

FIREBASE DATABASES ANALYSIS

| TITLE | SEVERITY | DESCRIPTION |
|----------------------------------|----------|--|
| App talks to a Firebase database | info | The app talks to Firebase database at https://iaccess-innovations-inc.firebaseio.com |
| Firebase Remote Config disabled | secure | Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/120414179890/namespaces/firebase:fetch?key=AlzaSyBY5cU525pWqrA9ymWYKX57JLPkeNjFfQw. This is indicated by the response: {'state': 'NO_TEMPLATE'} |

ABUSED PERMISSIONS

| TYPE | MATCHES | PERMISSIONS |
|---------------------|---------|---|
| Malware Permissions | 9/25 | android.permission.INTERNET, android.permission.ACCESS_FINE_LOCATION, android.permission.GET_ACCOUNTS, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.ACCESS_COARSE_LOCATION, android.permission.WAKE_LOCK |

| TYPE | MATCHES | PERMISSIONS |
|--------------------------------|---------|--|
| Other Common Permissions | 2/44 | 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 |
|--|--------|---|
| iaccess-innovations-inc.firebaseio.com | ok | IP: 34.120.160.131 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|-----------------|--------|---|
| cdn.branch.io | ok | IP: 3.161.213.81 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map |
| www.apache.org | ok | IP: 151.101.2.132 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map |
| api2.branch.io | ok | IP: 3.161.213.3 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map |
| maps.google.com | ok | IP: 142.251.32.78 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---------------------|--------|---|
| www.googleapis.com | ok | IP: 142.251.32.74 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map |
| github.com | ok | IP: 140.82.112.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map |
| venues.iaccess.life | ok | IP: 172.64.80.1 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map |
| branch.app.link | ok | IP: 13.225.195.103 Country: Canada Region: Quebec City: Montreal Latitude: 45.508839 Longitude: -73.587807 View: Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|--------------------|--------|--|
| graph.facebook.com | ok | IP: 31.13.80.8 Country: Canada Region: Ontario City: Toronto Latitude: 43.700111 Longitude: -79.416298 View: Google Map |
| docs.branch.io | ok | IP: 13.225.195.72 Country: Canada Region: Quebec City: Montreal Latitude: 45.508839 Longitude: -73.587807 View: Google Map |
| play.google.com | ok | IP: 142.251.33.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map |
| api.branch.io | ok | IP: 13.225.195.57 Country: Canada Region: Quebec City: Montreal Latitude: 45.508839 Longitude: -73.587807 View: Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|-------------------------|--------|---|
| bnc.lt | ok | IP: 54.192.51.38 Country: United States of America Region: New York City: New York City Latitude: 40.714272 Longitude: -74.005966 View: Google Map |
| issuetracker.google.com | ok | IP: 142.251.41.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map |
| realm.io | ok | IP: 3.162.3.37 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map |
| maps.googleapis.com | ok | IP: 142.251.41.74 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map |

EMAILS

| EMAIL | FILE |
|---------------|---|
| help@realm.io | lib/x86_64/librealm-jni.so |
| help@realm.io | lib/mips/librealm-jni.so |
| help@realm.io | lib/armeabi-v7a/librealm-jni.so |
| help@realm.io | lib/arm64-v8a/librealm-jni.so |
| help@realm.io | lib/x86/librealm-jni.so |
| help@realm.io | apktool_out/lib/x86_64/librealm-jni.so |
| help@realm.io | apktool_out/lib/mips/librealm-jni.so |
| help@realm.io | apktool_out/lib/armeabi-v7a/librealm-jni.so |
| help@realm.io | apktool_out/lib/arm64-v8a/librealm-jni.so |
| help@realm.io | apktool_out/lib/x86/librealm-jni.so |

TRACKERS

| TRACKER | CATEGORIES | URL |
|---------|------------|-----|
|---------|------------|-----|

| TRACKER | CATEGORIES | URL |
|---------------------------|-----------------|---|
| Branch | Analytics | https://reports.exodus-privacy.eu.org/trackers/167 |
| Facebook Analytics | Analytics | https://reports.exodus-privacy.eu.org/trackers/66 |
| Facebook Login | Identification | https://reports.exodus-privacy.eu.org/trackers/67 |
| Facebook Places | | https://reports.exodus-privacy.eu.org/trackers/69 |
| Facebook Share | | https://reports.exodus-privacy.eu.org/trackers/70 |
| Google AdMob | Advertisement | https://reports.exodus-privacy.eu.org/trackers/312 |
| 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 |
|--|
| "email_or_username" : "Email" |
| "google_crash_reporting_api_key" : "AlzaSyBY5cU525pWqrA9ymWYKX57JLPkeNjFfQw" |
| "com_facebook_device_auth_instructions" : "facebook.com/device□□□□□□□□□□□□□□□□□□" |
| "firebase_database_url" : "https://iaccess-innovations-inc.firebaseio.com" |

| |
|--|
| POSSIBLE SECRETS |
| "google_maps_key" : "AlzaSyCnzZ7zud898lylG2n33m-yjD8kkvnhNT4" |
| "password" : "Password" |
| "google_api_key" : "AlzaSyBY5cU525pWqrA9ymWYKX57JLPkeNjFfQw" |
| "com_facebook_device_auth_instructions" : "□□facebook.com/device□□□□□□□□□□" |
| "com_facebook_device_auth_instructions" : "□□□facebook.com/device□□□□□□□□" |
| S2I+w5KEHsUH3LT7OhP0IPpiGbttsyfXS8OPgj9H8c= |
| AlzaSyDRKQ9d6kfsoZT2IUnZcZnBYvH69HEXNPE |
| 8jozaUbmU0+cz+Z2vGcXTqMyg+dqqRH4S6r1VoovLho= |
| 5nX3i9falmgAwp+vJrMG5SH4kaSgkg1lqURbpR8yu5CliYUoXxgGrqbeparJNzaH |
| aeXlk6U5mjj30buxy8Bq4aiVEx0vXK27OpzXGMIH06jfN+50MiGuLaWIDAfBuJ7L |
| n/zh5rj7xV8CKqQO4yT3YPkgscCCRhVRXB4t6q0Lln4MxQWb1+B3PzGHqxWsr5ZK |
| xjQBErXUAHP5Fiy2OGaxIsj1LRZnlXmD7KauDO7W9CY= |
| a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc |
| 39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319 |
| 4N++MHJG7DaqAGj5ekXoLt4z/TjCrBBrc9HCB45oQ0= |

| |
|---|
| POSSIBLE SECRETS |
| q1Q68gbSr2EunBKhtefssV0iPVsSUgl/oVqPT5EkVWWLAqn7uUnl8M9IRrc193ok |
| 115792089210356248762697446949407573529996955224135760342422259061068512044369 |
| XklO7OzRB/nYKluxj5R6ZFUOTX1+QVdOIRylIXZpNpTgXEtgHbFLDrp9Sw2pzLEm |
| XiXg1gP6ss3SGA7BxWDJoS/bsn+RZGya1xSqDPpM31M= |
| 9b8f518b086098de3d77736f9458a3d2f6f95a37 |
| b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef |
| acSXWqLoiDOa9iRZCInb7nh6aRhb1H6Ar4BZKXliXbQjT7xCSDUJQSYITLi7VRE3 |
| cc2751449a350f668590264ed76692694a80308a |
| PclTWSW2n3vILu55N/O6T6uvGoN3sb3ENUufScGURpJWiEgKkJPW5+de3HFzlp1o |
| EVJN/TCMZ7GKFXUn5FVqaiFpBuPpOILDGP3ulSHNpCXshXEpSNdbFKdWwHVuoFup |
| B3EEABB8EE11C2BE770B684D95219ECB |
| 258EAFa5-E914-47DA-95CA-C5AB0DC85B11 |
| 6mFBYTN64dqZuFHXYRjKBUcFVskXKkuG5eXtMJOzijl= |
| 6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151 |
| 54c42518-856a-44fb-aae0-cd6676d514e5 |

| |
|---|
| POSSIBLE SECRETS |
| ovD2w8qgKnhdjU64EGNB6VC/4TS2TT8Urb92jfjAbytu0IUzWJhztha6MlIntcfr |
| df6b721c8b4d3b6eb44c861d4415007e5a35fc95 |
| cgAKI3yZwPTLVG7tkL44jQX/NcvqAg3qlogimMrr39Y= |
| 5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b |
| vghXk3cKhthRTrGHEghRpAeUOOQ4rsXJlstQwRZFRSI= |
| 115792089210356248762697446949407573530086143415290314195533631308867097853951 |
| w2Yi1Oh/+ojvmOXI2j8V49D6I1wst7r+nL6ZGj9lxx4= |
| 4V37Zv/fqUn78vx5Tt2zbOoOKYn7HiwHmwoLsVX89T8= |
| 11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650 |
| 6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296 |
| 39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643 |
| 051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00 |
| 0220378AB1E5C05E6BABCBD8544FB3B7 |
| 2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3 |
| mTNK/hSVnW4n4RLzlp0zVO6EryuXJLOUcQEmjtjB9DUY112LUWWesswdZtMa7y6p |

| |
|---|
| POSSIBLE SECRETS |
| MKeQLb34PV6WvaQMmX+paFRUdARnA5uJeloPewslu7Y= |
| 0ABBF2A2B6DB7DBD7FAD7C5AF14F9D38 |
| E92CD5CD54A7A0A13721383CC985B72C |
| 6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449 |
| JBYNfhkoY+av96PAhHaYmh4ILl4Wz+5Dx4kUxGI7MKU= |
| 5e8f16062ea3cd2c4a0d547876baa6f38cabf625 |
| c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66 |
| u22PozhAGTsMYqYY9Itvps3brbQxztucPZcziRCNXgY= |
| SRbYMN68AMwZPDazOU0VwXZCPW/RYdycS0nF65kXvuU= |
| Dyw3YwormLeBtZ+Vho7wUteRBeDP0N4ERij37dwAhdsTa+AWlxo0cVJYu2sh+wM6Z |
| o3sCvRiU+Z55Vq2c5MFpXXz5zhAwK6As2YFncq0GyBE= |
| 6o7Euox9oMPrm+kDI dpZkcjz/I5IVbquuPy8q2o40i0= |
| dW/qTgfnk+N3jTeFG+isrkHYAmK5rvVNrAs0jV9mlQw+GJB5Wra2UekuWLdZk5+S |
| 8jNkyL0QcOh7+QT35sRux/OSBMCME2jK2jxuPwwdyiE= |
| 259utKoX96rcvfsLyw2B6DE/Q7VoxcKOsfNaFRI9Mtc= |

| |
|--|
| POSSIBLE SECRETS |
| WOShqhgr9S2+KWu9Egc6HFcn4swHmZFZtWqP6usmKaM= |
| gVM0JRg+DOkrsI9oCHxtH1dgXrNfriVsgZHgDDAoqJrGM375bLO+YYbLV1Zmqbos |
| UuLLTElpb3GapgO36wP979eOjuRqhTDS48Q5ODmGyn0= |
| aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7 |
| op5KBekVQPoxsxYX+X/7eh8kKEtGvOI4PsFUrqrr5uUqV8XPsfYFWjpcOqMo40LHh |
| 8a3c4b262d721acd49a4bf97d5213199c86fa2b9 |
| 4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5 |
| ZT3tAbBtTEtCq6QAxk0/ceVyLEGcahlxKWW1sq8eFajMNshmnssxr8BdGRJAdE4Rd |
| WOppAbmRFp5IFwVdOZEc11jI/CJHWcHpVC1YpMJ+670= |
| 0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78 |
| 7R+mfOkSNCrQtFB3YplnarFD7M+FEULIYquizu5+MUY= |
| lyQAFx+egrQVwFwmgo5MPWo4EwlxxTsBU9XR7kWqdGU3ZIVPubUx3i6napgz24Ej |
| QodYd1iiGym9GiGvy+5SEw8mM3D9A1zPjofiy0dxhPA= |
| YjzzQehJeCifZSNNQYt6AMI1PztKU4MnaH8NbKqcb2wt6Z2fkDf89WCDkbbB7WQ+R |
| 3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f |

| |
|--|
| POSSIBLE SECRETS |
| K3ciHTzfFv48jNbIfVE5dqZajsSALR7qTLK2cRbwd3U= |
| 470fa2b4ae81cd56ecbcd9735803434cec591fa |

PLAYSTORE INFORMATION

Title: iAccess Life - Accessibility

Score: 4.4848485 **Installs:** 5,000+ **Price:** 0 **Android Version Support:** **Category:** Lifestyle **Play Store URL:** [com.iaccessapp](https://play.google.com/store/apps/details?id=com.iaccessapp)

Developer Details: iAccess Innovations, iAccess+Innovations, None, <https://www.iaccess.life>, info@iaccess.life,

Release Date: Mar 18, 2019 **Privacy Policy:** [Privacy link](#)

Description:

iAccess Life is a platform designed out of an essential need to change the way our community accommodates those of us with physical limitations. We have designed this app to give users with a disabilities, wheelchair users, and users of mobility aides such as canes and walkers a platform for their voices to be heard, to share their experiences with accessibility at establishments around the world, and to find new and accessible places to visit and explore. iAccess Life is your disabled access guide as well as your platform to share your experiences with accessibility in public places. Whether you are paralyzed, suffer from a spinal cord injury or have experienced a health set back that requires you to use a wheelchair, cane, walker, crutches, etc. we feel that iAccess Life is an essential tool for your everyday life. As a disabled traveler or wheelchair traveler you can use iAccess Life to future plan by searching for accessible hotels, restaurants, stores, etc. that meet your accessibility needs with their accommodations. We encourage happiness, exploration and wanderlust. At iAccess we want to instill this type of energy into our users. Some users may come to us with all these qualities already ingrained in their DNA. Others may be looking to find their footing as they embark on a new journey. Our goal is to help everyone access life, as stress free as possible by being your guide to accessible events and venues. iAccess Life is for those ready to embark on a new adventure and an unforgettable experience. Through empowering users with mobility impairments, we hope to create an awareness around accessibility issues and how easily they can be addressed. We have a passion for creating moments and we want to be the catalyst for yours. Don't look for change, BE the change!

SCAN LOGS

| Timestamp | Event | Error |
|-----------|-------|-------|
|-----------|-------|-------|

| | | |
|---------------------|--|----|
| 2024-11-27 01:20:08 | Generating Hashes | OK |
| 2024-11-27 01:20:09 | Extracting APK | OK |
| 2024-11-27 01:20:09 | Unzipping | OK |
| 2024-11-27 01:20:09 | Getting Hardcoded Certificates/Keystores | OK |
| 2024-11-27 01:20:09 | Parsing APK with androguard | OK |
| 2024-11-27 01:20:11 | Parsing AndroidManifest.xml | OK |
| 2024-11-27 01:20:11 | Extracting Manifest Data | OK |
| 2024-11-27 01:20:11 | Manifest Analysis Started | OK |
| 2024-11-27 01:20:11 | Reading Network Security config from network_security_config.xml | OK |
| 2024-11-27 01:20:11 | Parsing Network Security config | OK |
| 2024-11-27 01:20:12 | Performing Static Analysis on: iAccess Life (com.iaccessapp) | OK |

| | | |
|---------------------|--|----|
| 2024-11-27 01:20:12 | Fetching Details from Play Store: com.iaccessapp | OK |
| 2024-11-27 01:20:12 | Checking for Malware Permissions | OK |
| 2024-11-27 01:20:12 | Fetching icon path | OK |
| 2024-11-27 01:20:12 | Library Binary Analysis Started | OK |
| 2024-11-27 01:20:12 | Analyzing lib/x86_64/librealm-jni.so | OK |
| 2024-11-27 01:20:12 | Analyzing lib/mips/librealm-jni.so | OK |
| 2024-11-27 01:20:12 | Analyzing lib/armeabi-v7a/librealm-jni.so | OK |
| 2024-11-27 01:20:12 | Analyzing lib/arm64-v8a/librealm-jni.so | OK |
| 2024-11-27 01:20:12 | Analyzing lib/x86/librealm-jni.so | OK |
| 2024-11-27 01:20:12 | Analyzing apktool_out/lib/x86_64/librealm-jni.so | OK |
| 2024-11-27 01:20:12 | Analyzing apktool_out/lib/mips/librealm-jni.so | OK |

| | | |
|---------------------|---|----|
| 2024-11-27 01:20:12 | Analyzing apktool_out/lib/armeabi-v7a/librealm-jni.so | OK |
| 2024-11-27 01:20:12 | Analyzing apktool_out/lib/arm64-v8a/librealm-jni.so | OK |
| 2024-11-27 01:20:12 | Analyzing apktool_out/lib/x86/librealm-jni.so | OK |
| 2024-11-27 01:20:12 | Reading Code Signing Certificate | OK |
| 2024-11-27 01:20:13 | Running APKiD 2.1.5 | OK |
| 2024-11-27 01:20:16 | Updating Trackers Database.... | OK |
| 2024-11-27 01:20:16 | Detecting Trackers | OK |
| 2024-11-27 01:20:18 | Decompiling APK to Java with JADX | OK |
| 2024-11-27 01:20:38 | Converting DEX to Smali | OK |
| 2024-11-27 01:20:39 | Code Analysis Started on - java_source | OK |
| 2024-11-27 01:20:40 | Android SBOM Analysis Completed | OK |

| | | |
|---------------------|---|----|
| 2024-11-27 01:20:45 | Android SAST Completed | OK |
| 2024-11-27 01:20:45 | Android API Analysis Started | OK |
| 2024-11-27 01:20:47 | Android API Analysis Completed | OK |
| 2024-11-27 01:20:47 | Android Permission Mapping Started | OK |
| 2024-11-27 01:20:48 | Android Permission Mapping Completed | OK |
| 2024-11-27 01:20:48 | Android Behaviour Analysis Started | OK |
| 2024-11-27 01:20:50 | Android Behaviour Analysis Completed | OK |
| 2024-11-27 01:20:50 | Extracting Emails and URLs from Source Code | OK |
| 2024-11-27 01:20:52 | Email and URL Extraction Completed | OK |
| 2024-11-27 01:20:52 | Extracting String data from APK | OK |
| 2024-11-27 01:20:52 | Extracting String data from SO | OK |

| | | |
|---------------------|--|----|
| 2024-11-27 01:20:52 | Extracting String data from Code | OK |
| 2024-11-27 01:20:52 | Extracting String values and entropies from Code | OK |
| 2024-11-27 01:20:54 | Performing Malware check on extracted domains | OK |
| 2024-11-27 01:20:56 | Saving to Database | OK |

Report Generated by - MobSF v4.2.6

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.