# MOBSF

# ANDROID STATIC ANALYSIS REPORT

SALTO Homelok (1.5.0)

| | |
|---|---|
| File Name: | com.saltosystems.android.homelok.apk |
| Package Name: | com.saltosystems.android.homelok |
| Scan Date: | Jan. 3, 2026, 6:09 a.m. |
| App Security Score: | 55/100 (MEDIUM RISK) |
| Grade: | B |
| Trackers Detection: | 2/432 |

# FINDINGS SEVERITY

| HIGH | MEDIUM | INFO | SECURE | HOTSPOT |
|---|---|---|---|---|
| 2 | 17 | 3 | 3 | 1 |

# FILE INFORMATION

**File Name:** com.saltosystems.android.homelok.apk
**Size:** 8.39MB
**MD5:** 9573bb861418606aa9375548646a532f
**SHA1:** 43bd769432515b0523c49b88e730f9446a94d474
**SHA256:** dabd592e49784428817781a82a1ce3a241bd875eca252a9d52f952bf2c07e404

# APP INFORMATION

**App Name:** SALTO Homelok
**Package Name:** com.saltosystems.android.homelok
**Main Activity:** com.saltosystems.android.homelok.ui.MainActivity
**Target SDK:** 33
**Min SDK:** 24
**Max SDK:**
**Android Version Name:** 1.5.0

**Android Version Code:** 10500900

# APP COMPONENTS

**Activities:** 3
**Services:** 12
**Receivers:** 15
**Providers:** 2
**Exported Activities:** 1
**Exported Services:** 3
**Exported Receivers:** 5
**Exported Providers:** 0

# CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
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: 2022-11-10 16:54:37+00:00
Valid To: 2052-11-10 16:54:37+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xa806961df6aefc7ae9e9b6965fe949b49b37469
Hash Algorithm: sha256
md5: bc4729a903b32ff843a766adc0a6f04b
sha1: 05d0783f2d4d27348d6247f1e8191a4455edd617
sha256: 2e9d7785f72c5860da3644ccf18a30f0cb593564bec86a5b6499806f8ead3201
sha512: 8657b7c9b9c0100ea4d8597dee2476810545d5ac4b072a3b0c0bbe14c4efa6d6bb7a75e52d8cafb9bad80b5b136e31dd4d6a2de024df88ea868a9a5d118f31e6
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: ca3c382e16b318d3bf0c8c0994cbcb7264ff6d1f101a9de7b78e5f24d1a1bef5
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.BLUETOOTH_CONNECT | dangerous | necessary for connecting to paired Bluetooth devices. | Required to be able to connect to paired Bluetooth devices. |
| android.permission.BLUETOOTH_SCAN | dangerous | required for discovering and pairing Bluetooth devices. | Required to be able to discover and pair nearby Bluetooth devices. |
| 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.ACCESS_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. |
| android.permission.BLUETOOTH | normal | create Bluetooth connections | Allows applications to connect to paired bluetooth devices. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
| --- | --- | --- | --- |
| android.permission.BLUETOOTH_ADMIN | normal | bluetooth administration | Allows applications to discover and pair bluetooth devices. |
| android.permission.WAKE_LOCK | normal | prevent phone from sleeping | Allows an application to prevent the phone from going to sleep. |
| com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE | normal | permission defined by google | A custom permission defined by Google. |
| 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.FOREGROUND_SERVICE | normal | enables regular apps to use Service.startForeground. | Allows a regular application to use Service.startForeground. |
| com.saltosystems.android.homelok.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION | unknown | Unknown permission | Unknown permission from android reference |
| android.permission.NFC | normal | control Near-Field Communication | Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
| --- | --- | --- | --- |
| android.permission.ACCESS_COARSE_LOCATION | dangerous | coarse (network-based) location | Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are. |
| android.permission.ACCESS_FINE_LOCATION | dangerous | fine (GPS) location | Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power. |

# 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<br>Build.MANUFACTURER check<br>Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check<br>Build.PRODUCT check<br>Build.HARDWARE check<br>Build.TAGS check<br>possible VM check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

| FILE | DETAILS |
| --- | --- |
| classes3.dex | <table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check<br>Build.TAGS check<br>possible ro.secure check</td></tr><tr><td>Compiler</td><td>r8</td></tr></table> |

# BROWSABLE ACTIVITIES

| ACTIVITY | INTENT |
| --- | --- |
| com.saltosystems.android.homelok.ui.MainActivity | Schemes: https://,<br>Hosts: homelok.saltosystems.com, dev.homelok.saltosystems.com,<br>Paths: /, |
| net.openid.appauth.RedirectUriReceiverActivity | Schemes: https://,<br>Hosts: homelok.saltosystems.com, dev.homelok.saltosystems.com,<br>Paths: /oauth2redirect, |

# NETWORK SECURITY

| NO | SCOPE | SEVERITY | DESCRIPTION |
| --- | --- | --- | --- |

# CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

| TITLE | SEVERITY | DESCRIPTION |
|---|---|---|
| Signed Application | info | Application is signed with a code signing certificate |

# MANIFEST ANALYSIS

HIGH: 1 | WARNING: 9 | INFO: 0 | SUPPRESSED: 0

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 1 | App can be installed on a vulnerable unpatched Android version<br>Android 7.0, [minSdk=24] | 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 | Activity (net.openid.appauth.RedirectUriReceiverActivity) is not Protected.<br>[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. |
| 3 | Broadcast Receiver (com.saltosystems.android.homelok.widget.WidgetOpenDoorSmall) is not Protected.<br>[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. |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 4 | Broadcast Receiver (com.saltosystems.android.homelok.widget.WidgetOpenDoorMedium) is not Protected.<br>[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. |
| 5 | Broadcast Receiver (com.saltosystems.android.homelok.widget.WidgetOpenDoorLarge) is not Protected.<br>[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 | Service (com.saltosystems.android.homelok.shared.domain.digitalkey.hce.HomelokHceService) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: android.permission.BIND_NFC_SERVICE<br>[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 | Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: android.permission.BIND_JOB_SERVICE<br>[android:exported=true] | warning | A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission. |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 8 | Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: android.permission.DUMP<br>[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. |
| 9 | Service (com.saltosystems.justinmobile.sdk.hce.JustinHceService) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: android.permission.BIND_NFC_SERVICE<br>[android:exported=true] | warning | A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission. |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 10 | Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: android.permission.DUMP<br>[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: 1 | WARNING: 6 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 1 | This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel. | secure | OWASP MASVS: MSTG-NETWORK-4 | ch/qos/logback/core/net/ssl/SSLContextFactoryBean.java<br>com/saltosystems/android/homelok/obscured/gi.java<br>com/saltosystems/android/homelok/obscured/kk2.java<br>com/saltosystems/android/homelok/obscured/wf2.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
| --- | --- | --- | --- | --- |
| 2 | The App uses an insecure Random Number Generator. | warning | CWE: CWE-330: Use of Insufficiently Random Values<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-6 | com/saltosystems/android/homelok/obscured/a03.java<br>com/saltosystems/android/homelok/obscured/b1.java<br>com/saltosystems/android/homelok/obscured/b13.java<br>com/saltosystems/android/homelok/obscured/dl0.java<br>com/saltosystems/android/homelok/obscured/ra0.java<br>com/saltosystems/android/homelok/obscured/rk2.java<br>com/saltosystems/android/homelok/obscured/se2.java<br>com/saltosystems/android/homelok/obscured/tg2.java<br>com/saltosystems/android/homelok/obscured/uj2.java<br>com/saltosystems/android/homelok/obscured/wj2.java<br>com/saltosystems/android/homelok/obscured/wl0.java |
| | | | | ch/qos/logback/classic/android/LogcatAppender.java<br>ch/qos/logback/classic/net/SimpleSocketServer.java<br>ch/qos/logback/classic/pattern/TargetLengthBasedClassNameAbbreviator.java<br>ch/qos/logback/classic/spi/ThrowableProxy.java<br>ch/qos/logback/core/joran/util/ConfigurationWatchListUtil.java<br>ch/qos/logback/core/net/DefaultSocketConnector.java<br>ch/qos/logback/core/net/SocketConnectorBase.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
| --- | --- | --- | --- | --- |
| | | | | ch/qos/logback/core/recovery/ResilientOutputStreamBase.java<br>ch/qos/logback/core/spi/ContextAwareBase.java<br>ch/qos/logback/core/spi/ContextAwareImpl.java<br>ch/qos/logback/core/subst/Node.java<br>com/airbnb/lottie/LottieAnimationView.java<br>com/saltosystems/android/homelok/obscured/ac.java<br>com/saltosystems/android/homelok/obscured/aw.java<br>com/saltosystems/android/homelok/obscured/bz3.java<br>com/saltosystems/android/homelok/obscured/c00.java<br>com/saltosystems/android/homelok/obscured/cl3.java<br>com/saltosystems/android/homelok/obscured/dt1.java<br>com/saltosystems/android/homelok/obscured/el3.java<br>com/saltosystems/android/homelok/obscured/et1.java<br>com/saltosystems/android/homelok/obscured/ez2.java<br>com/saltosystems/android/homelok/obscured/f4.java<br>com/saltosystems/android/homelok/obscured/fc.java<br>com/saltosystems/android/homelok/obscured/gf3.java<br>com/saltosystems/android/homelok/obscured/gq1.java<br>com/saltosystems/android/homelok/obscured/gt1.java<br>com/saltosystems/android/homelok/obscured/gz0.java<br>com/saltosystems/android/homelok/obsc |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
| --- | --- | --- | --- | --- |
| | | | | ured/h92.java<br>com/saltosystems/android/homelok/obsc<br>ured/hj2.java |
| 3 | The App logs information. Sensitive information should never be logged. | info | CWE: CWE-532: Insertion of Sensitive Information into Log File<br>OWASP MASVS: MSTG-STORAGE-3 | com/saltosystems/android/homelok/obsc<br>ured/hp3.java<br>com/saltosystems/android/homelok/obsc<br>ured/hz2.java<br>com/saltosystems/android/homelok/obsc<br>ured/i11.java<br>com/saltosystems/android/homelok/obsc<br>ured/ip3.java<br>com/saltosystems/android/homelok/obsc<br>ured/jp3.java<br>com/saltosystems/android/homelok/obsc<br>ured/jv0.java<br>com/saltosystems/android/homelok/obsc<br>ured/kz2.java<br>com/saltosystems/android/homelok/obsc<br>ured/mr1.java<br>com/saltosystems/android/homelok/obsc<br>ured/nf3.java<br>com/saltosystems/android/homelok/obsc<br>ured/np3.java<br>com/saltosystems/android/homelok/obsc<br>ured/nu0.java<br>com/saltosystems/android/homelok/obsc<br>ured/oy3.java<br>com/saltosystems/android/homelok/obsc<br>ured/pb.java<br>com/saltosystems/android/homelok/obsc<br>ured/q82.java<br>com/saltosystems/android/homelok/obsc<br>ured/qj3.java<br>com/saltosystems/android/homelok/obsc<br>ured/qm3.java<br>com/saltosystems/android/homelok/obsc<br>ured/r13.java<br>com/saltosystems/android/homelok/obsc<br>ured/rj3.java<br>com/saltosystems/android/homelok/obsc |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
| --- | --- | --- | --- | --- |
| | | | | ured/rv.java<br>com/saltosystems/android/homelok/obsc<br>ured/rz.java<br>com/saltosystems/android/homelok/obsc<br>ured/s03.java<br>com/saltosystems/android/homelok/obsc<br>ured/sa.java<br>com/saltosystems/android/homelok/obsc<br>ured/ss.java<br>com/saltosystems/android/homelok/obsc<br>ured/sw3.java<br>com/saltosystems/android/homelok/obsc<br>ured/ta.java<br>com/saltosystems/android/homelok/obsc<br>ured/tb.java<br>com/saltosystems/android/homelok/obsc<br>ured/u04.java<br>com/saltosystems/android/homelok/obsc<br>ured/u42.java<br>com/saltosystems/android/homelok/obsc<br>ured/u5.java<br>com/saltosystems/android/homelok/obsc<br>ured/uu3.java<br>com/saltosystems/android/homelok/obsc<br>ured/uw3.java<br>com/saltosystems/android/homelok/obsc<br>ured/vf3.java<br>com/saltosystems/android/homelok/obsc<br>ured/vk0.java<br>com/saltosystems/android/homelok/obsc<br>ured/vm2.java<br>com/saltosystems/android/homelok/obsc<br>ured/vp2.java<br>com/saltosystems/android/homelok/obsc<br>ured/vr.java<br>com/saltosystems/android/homelok/obsc<br>ured/vt0.java<br>com/saltosystems/android/homelok/obsc<br>ured/w42.java<br>com/saltosystems/android/homelok/obsc |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
| --- | --- | --- | --- | --- |
| | | | | ured/w5.java<br>com/saltosystems/android/homelok/obscured/w71.java<br>com/saltosystems/android/homelok/obscured/wb.java<br>com/saltosystems/android/homelok/obscured/wh3.java<br>com/saltosystems/android/homelok/obscured/wx3.java<br>com/saltosystems/android/homelok/obscured/x80.java<br>com/saltosystems/android/homelok/obscured/x91.java<br>com/saltosystems/android/homelok/obscured/xw3.java<br>com/saltosystems/android/homelok/obscured/y42.java<br>com/saltosystems/android/homelok/obscured/y62.java<br>com/saltosystems/android/homelok/obscured/yk3.java<br>com/saltosystems/android/homelok/obscured/zk3.java<br>net/openid/appauth/internal/Logger.java<br>org/slf4j/helpers/Util.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
| --- | --- | --- | --- | --- |
| 4 | Files may contain hardcoded sensitive information like usernames, passwords, keys etc. | warning | CWE: CWE-312: Cleartext Storage of Sensitive Information<br>OWASP Top 10: M9: Reverse Engineering<br>OWASP MASVS: MSTG-STORAGE-14 | ch/qos/logback/classic/joran/action/ConfigurationAction.java<br>ch/qos/logback/classic/sift/ContextBasedDiscriminator.java<br>ch/qos/logback/core/CoreConstants.java<br>ch/qos/logback/core/net/ssl/SSL.java<br>ch/qos/logback/core/rolling/helper/DateTokenConverter.java<br>ch/qos/logback/core/rolling/helper/IntegerTokenConverter.java<br>com/saltosystems/android/homelok/model/device/v1/WifiSettings.java<br>com/saltosystems/android/homelok/model/user/v1/User.java<br>com/saltosystems/android/homelok/model/wellknown/WellKnownData.java<br>com/saltosystems/android/homelok/obscured/am3.java<br>com/saltosystems/android/homelok/obscured/az0.java<br>com/saltosystems/android/homelok/obscured/es3.java<br>com/saltosystems/android/homelok/obscured/fm2.java<br>com/saltosystems/android/homelok/obscured/hi2.java<br>com/saltosystems/android/homelok/obscured/m42.java<br>com/saltosystems/android/homelok/obscured/qf0.java<br>com/saltosystems/android/homelok/obscured/uy0.java<br>com/saltosystems/android/homelok/ui/users/edit/keys/a.java<br>net/openid/appauth/ClientSecretPost.java<br>net/openid/appauth/RegistrationResponse.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | | net/openid/appauth/TokenRequest.java |
| 5 | App can read/write to External Storage. Any App can read data written to External Storage. | warning | CWE: CWE-276: Incorrect Default Permissions<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | ch/qos/logback/core/android/AndroidContextUtil.java |
| 6 | Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks | high | CWE: CWE-295: Improper Certificate Validation<br>OWASP Top 10: M3: Insecure Communication<br>OWASP MASVS: MSTG-NETWORK-3 | com/saltosystems/android/homelok/obscured/j7.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/saltosystems/android/homelok/ui/users/edit/keys/EditUserKeysViewModel.java |
| 8 | App can write to App Directory. Sensitive Information should be encrypted. | info | CWE: CWE-276: Incorrect Default Permissions<br>OWASP MASVS: MSTG-STORAGE-14 | com/saltosystems/android/homelok/shared/auth/AuthConfiguration.java |
| 9 | 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')<br>OWASP Top 10: M7: Client Code Quality | ch/qos/logback/classic/android/SQLiteAppender.java<br>com/saltosystems/android/homelok/obscured/iv0.java |
| 10 | This App may have root detection capabilities. | secure | OWASP MASVS: MSTG-RESILIENCE-1 | com/saltosystems/android/homelok/obscured/w03.java |
| 11 | This App may request root (Super User) privileges. | warning | CWE: CWE-250: Execution with Unnecessary Privileges<br>OWASP MASVS: MSTG-RESILIENCE-1 | com/saltosystems/android/homelok/obscured/jv.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 12 | App creates temp file. Sensitive information should never be written into a temp file. | warning | CWE: CWE-276: Incorrect Default Permissions<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | com/saltosystems/android/homelok/obscured/r13.java |

# NIAP ANALYSIS v1.3

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

# BEHAVIOUR ANALYSIS

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

| RULE ID | BEHAVIOUR | LABEL | FILES |
| --- | --- | --- | --- |
| 00022 | Open a file from given absolute path of the file | file | ch/qos/logback/classic/android/SQLiteAppender.java<br>ch/qos/logback/core/FileAppender.java<br>ch/qos/logback/core/android/AndroidContextUtil.java<br>ch/qos/logback/core/rolling/helper/Compressor.java<br>ch/qos/logback/core/rolling/helper/FileFinder.java<br>ch/qos/logback/core/rolling/helper/RenameUtil.java<br>com/saltosystems/android/homelok/obscured/db2.java<br>com/saltosystems/android/homelok/obscured/f03.java<br>com/saltosystems/android/homelok/obscured/gv3.java<br>com/saltosystems/android/homelok/obscured/jv0.java<br>com/saltosystems/android/homelok/obscured/la2.java<br>com/saltosystems/android/homelok/obscured/nl0.java<br>com/saltosystems/android/homelok/obscured/r13.java<br>com/saltosystems/android/homelok/obscured/vm2.java<br>com/saltosystems/android/homelok/obscured/vs2.java<br>io/realm/e.java<br>io/realm/internal/OsRealmConfig.java<br>io/realm/internal/OsSharedRealm.java<br>io/realm/internal/Util.java |
| 00013 | Read file and put it into a stream | file | ch/qos/logback/core/joran/GenericConfigurator.java<br>ch/qos/logback/core/joran/action/PropertyAction.java<br>ch/qos/logback/core/rolling/helper/Compressor.java<br>ch/qos/logback/core/util/FileUtil.java<br>com/saltosystems/android/homelok/obscured/cf2.java<br>com/saltosystems/android/homelok/obscured/db2.java<br>com/saltosystems/android/homelok/obscured/fc.java<br>com/saltosystems/android/homelok/obscured/g00.java<br>com/saltosystems/android/homelok/obscured/hp3.java<br>com/saltosystems/android/homelok/obscured/la2.java<br>com/saltosystems/android/homelok/obscured/lg0.java<br>com/saltosystems/android/homelok/obscured/np3.java<br>com/saltosystems/android/homelok/obscured/r13.java<br>com/saltosystems/android/homelok/obscured/vk0.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
| --- | --- | --- | --- |
| 00091 | Retrieve data from broadcast | collection | com/saltosystems/android/homelok/ui/keys/KeysFragment.java<br>net/openid/appauth/AuthorizationManagementActivity.java |
| 00036 | Get resource file from res/raw directory | reflection | com/saltosystems/android/homelok/obscured/dz2.java<br>com/saltosystems/android/homelok/obscured/gf3.java<br>com/saltosystems/android/homelok/obscured/u5.java<br>com/saltosystems/android/homelok/shared/auth/AuthConfiguration.java |
| 00114 | Create a secure socket connection to the proxy address | network command | com/saltosystems/android/homelok/obscured/kt2.java |
| 00026 | Method reflection | reflection | com/saltosystems/android/homelok/obscured/fc1.java<br>com/saltosystems/android/homelok/obscured/gc1.java |
| 00012 | Read data and put it into a buffer stream | file | ch/qos/logback/core/rolling/helper/Compressor.java<br>ch/qos/logback/core/util/FileUtil.java<br>com/saltosystems/android/homelok/obscured/vk0.java |
| 00173 | Get bounds in screen of an AccessibilityNodeInfo and perform action | accessibility service | com/saltosystems/android/homelok/obscured/f4.java |
| 00147 | Get the time of current location | collection location | com/saltosystems/android/homelok/obscured/qm3.java |
| 00075 | Get location of the device | collection location | com/saltosystems/android/homelok/obscured/qm3.java |
| 00115 | Get last known location of the device | collection location | com/saltosystems/android/homelok/obscured/qm3.java |
| 00189 | Get the content of a SMS message | sms | com/saltosystems/android/homelok/obscured/hq0.java |
| 00188 | Get the address of a SMS message | sms | com/saltosystems/android/homelok/obscured/hq0.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00200 | Query data from the contact list | collection contact | com/saltosystems/android/homelok/obscured/hq0.java |
| 00187 | Query a URI and check the result | collection sms calllog calendar | com/saltosystems/android/homelok/obscured/hq0.java |
| 00201 | Query data from the call log | collection calllog | com/saltosystems/android/homelok/obscured/hq0.java |
| 00077 | Read sensitive data(SMS, CALLLOG, etc) | collection sms calllog calendar | com/saltosystems/android/homelok/obscured/hq0.java |
| 00063 | Implicit intent(view a web page, make a phone call, etc.) | control | com/saltosystems/android/homelok/obscured/ol0.java<br>com/saltosystems/android/homelok/obscured/u5.java<br>com/saltosystems/android/homelok/shared/auth/AuthConfiguration.java<br>com/saltosystems/android/homelok/ui/users/edit/keys/EditUserKeysViewModel.java<br>net/openid/appauth/AuthorizationException.java |
| 00051 | Implicit intent(view a web page, make a phone call, etc.) via setData | control | com/saltosystems/android/homelok/obscured/u5.java<br>com/saltosystems/android/homelok/shared/auth/AuthConfiguration.java |
| 00123 | Save the response to JSON after connecting to the remote server | network command | net/openid/appauth/AuthorizationServiceConfiguration.java |
| 00162 | Create InetSocketAddress object and connecting to it | socket | com/saltosystems/android/homelok/obscured/kk2.java<br>com/saltosystems/android/homelok/obscured/o7.java |
| 00163 | Create new Socket and connecting to it | socket | com/saltosystems/android/homelok/obscured/kk2.java<br>com/saltosystems/android/homelok/obscured/o7.java |
| 00191 | Get messages in the SMS inbox | sms | com/saltosystems/android/homelok/obscured/gf3.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00079 | Hide the current app's icon | evasion | com/saltosystems/android/homelok/obscured/nh2.java |
| 00039 | Start a web server | control network | ch/qos/logback/classic/net/SimpleSocketServer.java |
| 00096 | Connect to a URL and set request method | command network | com/saltosystems/android/homelok/obscured/z20.java<br>net/openid/appauth/AuthorizationService.java |
| 00089 | Connect to a URL and receive input stream from the server | command network | net/openid/appauth/AuthorizationService.java |
| 00109 | Connect to a URL and get the response code | network command | net/openid/appauth/AuthorizationService.java |
| 00030 | Connect to the remote server through the given URL | network | com/saltosystems/android/homelok/obscured/z20.java |

# FIREBASE DATABASES ANALYSIS

| TITLE | SEVERITY | DESCRIPTION |
|---|---|---|
| Firebase Remote Config disabled | secure | Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/1001076883823/namespaces/firebase:fetch?key=AIzaSyDE9e7BQVApsvtY_oejrkZXIaHFYZR2KEI. This is indicated by the response: {'state': 'NO_TEMPLATE'} |

# ABUSED PERMISSIONS

| TYPE | MATCHES | PERMISSIONS |
|---|---|---|
| Malware Permissions | 8/25 | android.permission.INTERNET, android.permission.VIBRATE, android.permission.CAMERA, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION |
| Other Common Permissions | 4/44 | android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_SERVICE |

### Malware Permissions:
Top permissions that are widely abused by known malware.
### Other Common Permissions:
Permissions that are commonly abused by known malware.

# ! OFAC SANCTIONED COUNTRIES

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

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

# DOMAIN MALWARE CHECK

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|

| DOMAIN | STATUS | GEOLOCATION |
| --- | --- | --- |
| saltosystems.com | ok | **IP:** 151.101.2.133<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| issuetracker.google.com | ok | **IP:** 142.250.217.174<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| ns.adobe.com | ok | No Geolocation information available. |
| logback.qos.ch | ok | **IP:** 159.100.250.151<br>**Country:** Switzerland<br>**Region:** Vaud<br>**City:** Lausanne<br>**Latitude:** 46.515999<br>**Longitude:** 6.632820<br>**View:** Google Map |
| docs.mongodb.com | ok | **IP:** 3.33.186.135<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
| --- | --- | --- |
| www.slf4j.org | ok | **IP:** 31.97.181.89<br>**Country:** United Kingdom of Great Britain and Northern Ireland<br>**Region:** England<br>**City:** Bowness-on-Windermere<br>**Latitude:** 54.363312<br>**Longitude:** -2.918590<br>**View:** Google Map |
| www.w3.org | ok | **IP:** 104.18.22.19<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| support.saltosystems.com | ok | **IP:** 151.101.130.133<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| schemas.android.com | ok | No Geolocation information available. |
| xml.org | ok | **IP:** 104.239.142.8<br>**Country:** United States of America<br>**Region:** Texas<br>**City:** Windcrest<br>**Latitude:** 29.499678<br>**Longitude:** -98.399246<br>**View:** Google Map |

# TRACKERS

| TRACKER | CATEGORIES | URL |
| --- | --- | --- |
| 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 |
| --- |
| "google_api_key" : "AIzaSyDE9e7BQVApsvtY_oejrkZXIaHFYZR2KEI" |
| "google_crash_reporting_api_key" : "AIzaSyDE9e7BQVApsvtY_oejrkZXIaHFYZR2KEI" |
| "user_card_key_title" : "Key" |
| 5181942b9ebc31ce68dacb56c16fd79f |
| 6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151 |
| 470fa2b4ae81cd56ecbcda9735803434cec591fa |
| B6E60002-E2E3-BC82-4C72-929D0D29CA17 |
| B6E60003-E2E3-BC82-4C72-929D0D29CA17 |

| POSSIBLE SECRETS |
| --- |
| 4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5 |
| B6E60001-E2E3-BC82-4C72-929D0D29CA17 |
| ae2044fb577e65ee8bb576ca48a2f06e |
| 115792089210356248762697446949407573530086143415290314195533631308867097853951 |
| c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66 |
| aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7 |
| 7fmduHKTdHHrlMvldlEqAIlSfii1tl35bxj1OXN5Ve8c4lU6URVu4xtSHc3BVZxS6WWJnxMDhIfQN0N0K2NDJg== |
| ABi2fbt8vkzj7SJ8aD5jc4xJFTDFntdkMrYXL3itsvqY1QIw |
| 115792089210356248762697446949407573529996955224135760342422259061068512044369 |
| 5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b |
| 6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449 |
| b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef |
| 051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00 |
| 16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a |
| dZozdop5rgKNxjbrQAd5nntAGpgh9w84O1Xgg== |

| POSSIBLE SECRETS |
| --- |
| 3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f |
| 11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650 |
| 6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296 |
| 3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319 |
| 3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3 |

# PLAYSTORE INFORMATION

**Title:** Salto Homelok

**Score:** None **Installs:** 10,000+ **Price:** 0 **Android Version Support:** **Category:** Lifestyle **Play Store URL:** com.saltosystems.android.homelok

**Developer Details:** Salto Systems S.L., Salto+Systems+S.L., None, https://saltosystems.com/en/solutions/salto-homelok/, android@saltosystems.com,

**Release Date:** Nov 10, 2022 **Privacy Policy:** Privacy link

**Description:**

Salto Homelok smart access solution allows residents to efficiently manage access to their living space while enjoying a better keyless and mobile experience. Salto Homelok enables modern keyless living for residents, streamlines operations for managers and owners, and improves security across all types of residential properties. Our ground-breaking cloud smart access platform with intelligent, wire-free and virtually networked electronic locking SVN technology optimises hybrid deployments and enables the smart building ecosystem with no need of infrastructure. Homelok offers flexible, convenient smart access solutions for residential properties, connecting SALTO access control hardware to security infrastructure and to the property operations to manage any access point, in any type of building.

# SCAN LOGS

| Timestamp | Event | Error |
| --- | --- | --- |
| 2026-01-03 06:09:41 | Generating Hashes | OK |
| 2026-01-03 06:09:41 | Extracting APK | OK |
| 2026-01-03 06:09:41 | Unzipping | OK |
| 2026-01-03 06:09:41 | Parsing APK with androguard | OK |
| 2026-01-03 06:09:41 | Extracting APK features using aapt/aapt2 | OK |
| 2026-01-03 06:09:41 | Getting Hardcoded Certificates/Keystores | OK |
| 2026-01-03 06:09:42 | Parsing AndroidManifest.xml | OK |
| 2026-01-03 06:09:42 | Extracting Manifest Data | OK |
| 2026-01-03 06:09:42 | Manifest Analysis Started | OK |
| 2026-01-03 06:09:42 | Performing Static Analysis on: SALTO Homelok (com.saltosystems.android.homelok) | OK |

| | | |
|---|---|---|
| 2026-01-03 06:09:42 | Fetching Details from Play Store: com.saltosystems.android.homelok | OK |
| 2026-01-03 06:09:43 | Checking for Malware Permissions | OK |
| 2026-01-03 06:09:43 | Fetching icon path | OK |
| 2026-01-03 06:09:43 | Library Binary Analysis Started | OK |
| 2026-01-03 06:09:43 | Reading Code Signing Certificate | OK |
| 2026-01-03 06:09:43 | Running APKiD 3.0.0 | OK |
| 2026-01-03 06:09:45 | Detecting Trackers | OK |
| 2026-01-03 06:09:46 | Decompiling APK to Java with JADX | OK |
| 2026-01-03 06:09:54 | Converting DEX to Smali | OK |
| 2026-01-03 06:09:55 | Code Analysis Started on - java_source | OK |
| 2026-01-03 06:09:55 | Android SBOM Analysis Completed | OK |

| | | |
|---|---|---|
| 2026-01-03 06:09:58 | Android SAST Completed | OK |
| 2026-01-03 06:09:58 | Android API Analysis Started | OK |
| 2026-01-03 06:09:59 | Android API Analysis Completed | OK |
| 2026-01-03 06:09:59 | Android Permission Mapping Started | OK |
| 2026-01-03 06:10:01 | Android Permission Mapping Completed | OK |
| 2026-01-03 06:10:01 | Android Behaviour Analysis Started | OK |
| 2026-01-03 06:10:03 | Android Behaviour Analysis Completed | OK |
| 2026-01-03 06:10:03 | Extracting Emails and URLs from Source Code | OK |
| 2026-01-03 06:10:06 | Email and URL Extraction Completed | OK |
| 2026-01-03 06:10:06 | Extracting String data from APK | OK |
| 2026-01-03 06:10:06 | Extracting String data from Code | OK |

| | | |
|---|---|---|
| 2026-01-03 06:10:06 | Extracting String values and entropies from Code | OK |
| 2026-01-03 06:10:07 | Performing Malware check on extracted domains | OK |
| 2026-01-03 06:10:11 | Saving to Database | OK |

---

## Report Generated by - MobSF v4.4.4

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.