# MOBSF

## ANDROID STATIC ANALYSIS REPORT

Antivirus, Super Cleaner (1.5)

| | |
|---|---|
| File Name: | all1.apk |
| Package Name: | com.abbondioendrizzi.antivirus.supercleaner |
| Scan Date: | May 24, 2022, 9:57 a.m. |
| App Security Score: | 45/100 (MEDIUM RISK) |
| Grade: |  |

# FINDINGS SEVERITY

| HIGH | MEDIUM | INFO | SECURE | HOTSPOT |
|---|---|---|---|---|
| 5 | 18 | 1 | 2 | 1 |

# FILE INFORMATION

**File Name:** all1.apk
**Size:** 14.12MB
**MD5:** 1f32aa3ad68eac774cfcaeb0cd84de4d
**SHA1:** 512f378b8821064d5b48ceb0624dd17eca673667
**SHA256:** a56dacc093823dc1d266d68ddfba04b2265e613dcc4b69f350873b485b9e1f1c

# APP INFORMATION

**App Name:** Antivirus, Super Cleaner
**Package Name:** com.abbondioendrizzi.antivirus.supercleaner
**Main Activity:** com.abbondioendrizzi.antivirus.supercleaner.screen.main.MainActivity
**Target SDK:** 30
**Min SDK:** 26
**Max SDK:**
**Android Version Name:** 1.5
**Android Version Code:** 5

# APP COMPONENTS

Activities: 38
Services: 12
Receivers: 17
Providers: 3
Exported Activities: 0
Exported Services: 3
Exported Receivers: 7
Exported Providers: 0

# CERTIFICATE INFORMATION

APK is signed
v1 signature: False
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-01-29 11:40:42+00:00
Valid To: 2052-01-29 11:40:42+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xcb81bbca19b19f0628aecb9b1a61f6e1aad1b5b5
Hash Algorithm: sha256
md5: efab83ed3aa18f7326d093b13a8155ed
sha1: 7ff554b2fc5b9e34ed703b1b13e833f62363f459
sha256: b577daf82485cfd0c54cf6099bdd4d6ccb5061cb9b5eb41f3fac61b07d761da7
sha512: 6905df18b645aefc2174bea6597f694d9c275466593ef909c54c616511775eaca5de2644909b53e64441302183902894 7f1e1c2551d54ae3c224f5641326b55c
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 2ab8b6d7fd9aef4c7e2ac99c0bad0f0fb9b7692d553dc5d3fd7af8250c46ec0f

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

# APPLICATION PERMISSIONS

| PERMISSION | STATUS | INFO | DESCRIPTION |
| --- | --- | --- | --- |
| android.permission.BLUETOOTH | normal | create Bluetooth connections | Allows applications to connect to paired bluetooth devices. |
| android.permission.BLUETOOTH_ADMIN | normal | bluetooth administration | Allows applications to discover and pair bluetooth devices. |
| android.permission.CHANGE_WIFI_STATE | normal | change Wi-Fi status | Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks. |
| android.permission.KILL_BACKGROUND_PROCESSES | normal | kill background processes | Allows an application to kill background processes of other applications, even if memory is not low. |
| 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.FOREFGROUND_SERVICE | unknown | Unknown permission | Unknown permission from android reference |

| PERMISSION | STATUS | INFO | DESCRIPTION |
| --- | --- | --- | --- |
| android.permission.SYSTEM_ALERT_WINDOW | dangerous | display system-level alerts | Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone. |
| android.permission.WRITE_SYNC_SETTINGS | normal | write sync settings | Allows an application to modify the sync settings, such as whether sync is enabled for Contacts. |
| com.android.launcher.permission.INSTALL_SHORTCUT | unknown | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS_NOTIFICATION_POLICY | normal | | Marker permission for applications that wish to access notification policy. |
| android.permission.REQUEST_DELETE_PACKAGES | normal | | Allows an application to request deleting packages. |
| android.permission.WAKE_LOCK | normal | prevent phone from sleeping | Allows an application to prevent the phone from going to sleep. |
| android.permission.GET_PACKAGE_SIZE | normal | measure application storage space | Allows an application to find out the space used by any package. |
| 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.QUICKBOOT_POWERON | unknown | Unknown permission | Unknown permission from android reference |
| android.permission.CLEAR_APP_CACHE | SignatureOrSystem | delete all application cache data | Allows an application to free phone storage by deleting files in application cache directory. Access is usually very restricted to system process. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
| --- | --- | --- | --- |
| android.permission.WRITE_SETTINGS | dangerous | modify global system settings | Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration. |
| android.permission.INTERNET | normal | full Internet access | Allows an application to create network sockets. |
| android.permission.REQUEST_INSTALL_PACKAGES | dangerous | Allows an application to request installing packages. | Malicious applications can use this to try and trick users into installing additional malicious packages. |
| android.permission.GET_TASKS | dangerous | retrieve running applications | Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications. |
| android.permission.PACKAGE_USAGE_STATS | signature | update component usage statistics | Allows the modification of collected component usage statistics. Not for use by common applications. |
| android.permission.FOREGROUND_SERVICE | normal | | Allows a regular application to use Service.startForeground. |
| 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.USE_FINGERPRINT | normal | allow use of fingerprint | This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead. |
| android.permission.ACCESS_WIFI_STATE | normal | view Wi-Fi status | Allows an application to view the information about the status of Wi-Fi. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
| --- | --- | --- | --- |
| android.permission.RECEIVE_USER_PRESENT | unknown | Unknown permission | Unknown permission from android reference |
| android.permission.CHANGE_NETWORK_STATE | normal | change network connectivity | Allows applications to change network connectivity state. |
| android.permission.SET_WALLPAPER | normal | set wallpaper | Allows the application to set the system wallpaper. |
| android.permission.VIBRATE | normal | control vibrator | Allows the application to control the vibrator. |
| android.permission.QUERY_ALL_PACKAGES | normal | | Allows query of any normal app on the device, regardless of manifest declarations. |
| android.permission.ACCESS_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. |

# APKID ANALYSIS

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

| FILE | DETAILS |
| --- | --- |
| classes.dex | <table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check<br>Build.MODEL check<br>Build.MANUFACTURER check<br>Build.PRODUCT check</td></tr><tr><td>Compiler</td><td>r8</td></tr></table> |

## NETWORK SECURITY

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

## MANIFEST ANALYSIS

| NO | ISSUE | SEVERITY | DESCRIPTION |
| --- | --- | --- | --- |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 1 | Clear text traffic is Enabled For App [android:usesCleartextTraffic=true] | high | The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected. |
| 2 | Application Data can be Backed up [android:allowBackup=true] | warning | This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device. |
| 3 | Service (com.abbondioendrizzi.antivirus.supercleaner.service.ForceStopAccessibility) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true] | warning | A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission. |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 4 | Service (com.abbondioendrizzi.antivirus.supercleaner.api.NotificationListener) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: android.permission.BIND_NOTIFICATION_LISTENER_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. |
| 5 | Broadcast Receiver (com.abbondioendrizzi.antivirus.supercleaner.receiver.AlarmReceiver) is not Protected.<br>An intent-filter exists. | 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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported. |
| 6 | Broadcast Receiver (com.abbondioendrizzi.antivirus.supercleaner.lock.receiver.LockRestarterBroadcastReceiver) is not Protected.<br>[android:exported=true] | high | A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. |
| 7 | Broadcast Receiver (com.abbondioendrizzi.antivirus.supercleaner.lock.receiver.BootBroadcastReceiver) is not Protected.<br>An intent-filter exists. | 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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported. |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 8 | Broadcast Receiver (com.abbondioendrizzi.antivirus.supercleaner.receiver.AutoRebootReceiver) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: android.permission.RECEIVE_BOOT_COMPLETED<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 | Broadcast Receiver (com.security.applock.service.receiver.WidgetReceiver) is not Protected.<br>An intent-filter exists. | 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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported. |
| 10 | Broadcast Receiver (com.security.applock.service.receiver.RestarterBroadcastReceiver) is not Protected.<br>[android:exported=true] | high | A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 11 | Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked.<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. |
| 12 | 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. |
| 13 | High Intent Priority (99999)<br>[android:priority] | warning | By setting an intent priority higher than another intent, the app effectively overrides other requests. |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 14 | High Intent Priority (1000)<br>[android:priority] | warning | By setting an intent priority higher than another intent, the app effectively overrides other requests. |

# </> CODE ANALYSIS

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | | d/d/a/n/s.java<br>d/d/a/m/w/c/r.java<br>b/h/l/e.java<br>b/b/h/h.java<br>b/u/f.java<br>b/f/c/b.java<br>com/makeramen/roundedimageview/RoundedImageView.java<br>b/s/a.java<br>b/n/b/j0.java<br>b/h/b/m.java<br>b/b/g/i/g.java<br>d/d/a/n/e.java<br>d/d/a/m/w/c/b0.java<br>b/c0/e.java<br>b/b/g/i/d.java<br>b/b/h/y.java<br>b/b/h/p0.java<br>d/d/a/m/w/c/j.java<br>b/n/b/l0.java<br>b/u/i.java<br>d/d/a/m/u/l.java<br>d/d/a/m/u/e0/a.java<br>b/b/h/k0.java<br>b/m/a/a.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
| --- | --- | --- | --- | --- |
| | | | | b/n/b/m.java<br>b/n/b/e.java<br>d/d/a/m/v/f.java<br>d/d/a/m/t/l.java<br>d/d/a/m/v/t.java<br>d/d/a/m/w/a.java<br>d/d/a/m/w/g/j.java<br>b/j/b/f.java<br>d/l/a/f.java<br>d/d/a/m/w/c/k.java<br>b/b/c/k.java<br>b/c0/j.java<br>b/n/b/l.java<br>b/u/e.java<br>b/n/b/z0.java<br>b/n/b/c.java<br>d/d/a/m/w/c/z.java<br>d/d/a/n/o.java<br>b/h/d/d.java<br>b/c0/u/a.java<br>d/j/a/j.java<br>b/n/b/f0.java<br>b/h/d/e.java<br>b/h/k/s.java<br>d/d/a/l/d.java<br>d/d/a/l/e.java<br>b/b/h/i.java<br>b/w/a/c.java<br>d/d/a/m/w/c/m.java<br>d/d/a/m/v/s.java<br>d/d/a/q/h.java<br>b/f/c/c.java<br>d/b/a/f0/c.java<br>b/f/b/d.java<br>b/h/c/b/f.java<br>d/d/a/m/v/d.java<br>b/b/h/c0.java<br>d/d/a/m/w/c/c.java<br>b/n/b/k0.java<br>b/b/c/h.java<br>d/d/a/b.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<br>OWASP MASVS: MSTG-STORAGE-3 | com/abbondioendrizzi/antivirus/supercleaner/lock/receiver/BootBroadcastReceiver.java<br>b/b/h/q0.java<br>d/d/a/m/u/c0/i.java<br>d/d/a/m/u/d0/e.java<br>d/d/a/m/u/i.java<br>d/g/a/a/c/g.java<br>b/b/h/x0.java<br>b/h/g/b.java<br>b/h/b/d.java<br>d/j/a/h.java<br>com/security/applock/service/AntiTheftService.java<br>d/d/a/i.java<br>d/d/a/m/w/g/a.java<br>h/l0/k/h.java<br>org/litepal/util/LogUtil.java<br>d/g/a/a/w/b.java<br>b/n/b/a1.java<br>d/d/a/m/w/g/d.java<br>d/d/a/m/t/o/b.java<br>b/h/k/a.java<br>b/b/c/t.java<br>d/d/a/m/u/r.java<br>d/o/a/k/a.java<br>d/d/a/q/j/i.java<br>d/d/a/s/k/a.java<br>d/i/a/b.java<br>d/d/a/m/u/d0/j.java<br>d/g/a/a/o/g.java<br>b/w/a/f/c.java<br>b/n/b/a.java<br>b/h/b/b.java<br>b/b/g/f.java<br>b/b/h/u.java<br>d/g/a/a/x/a.java<br>d/d/a/n/p.java<br>b/n/b/c0.java<br>b/i/a/b.java<br>b/b/h/i0.iava |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
| --- | --- | --- | --- | --- |
| | | | | d/d/a/m/u/b0.java<br>b/h/b/a0.java<br>b/a/g/d.java<br>b/s/u/a.java<br>b/h/b/c.java<br>d/d/a/m/t/b.java<br>b/b/h/l0.java<br>b/h/k/b.java<br>b/h/k/b0.java<br>com/security/applock/service/jobSchedul<br>er/JobSchedulerService.java<br>d/d/a/m/u/c0/j.java<br>b/b/h/q.java<br>d/d/a/m/u/j.java<br>d/m/a/h/f.java<br>b/f/c/d.java<br>d/d/a/m/w/c/n.java<br>d/d/a/m/t/j.java<br>h/l0/k/i/d.java<br>d/g/a/a/t/c.java<br>d/g/a/a/z/g.java<br>b/h/k/j.java<br>d/d/a/m/v/c.java<br>b/b/h/z0.java<br>b/s/u/b.java<br>d/d/a/h.java<br>b/x/y.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 | d/a/a/a/l/d.java<br>f/m/a.java<br>f/m/d/a.java<br>com/abbondioendrizzi/antivirus/supercleaner/service/ServiceManager.java<br>com/abbondioendrizzi/antivirus/supercleaner/screen/junkfile/JunkFileActivity.java<br>com/abbondioendrizzi/antivirus/supercleaner/screen/setting/SettingActivity.java<br>f/m/b.java<br>com/abbondioendrizzi/antivirus/supercleaner/screen/main/home/FragmentHome.java<br>b/a/g/d.java<br>com/abbondioendrizzi/antivirus/supercleaner/screen/gameboost/GameBoostActivity.java<br>d/a/a/a/c/d.java |
| 3 | MD5 is a weak hash known to have hash collisions. | warning | CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | d/a/a/a/l/d.java<br>com/abbondioendrizzi/antivirus/supercleaner/api/NotificationListener.java |
| 4 | App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database. | warning | CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')<br>OWASP Top 10: M7: Client Code Quality | org/litepal/crud/DataSupport.java<br>d/a/a/a/e/a.java<br>b/u/e.java<br>org/litepal/tablemanager/Generator.java<br>d/a/a/a/c/a.java<br>org/litepal/tablemanager/AssociationCreator.java<br>b/w/a/f/c.java<br>org/litepal/util/DBUtility.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 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 | d/a/a/a/j/s.java<br>d/o/a/l/a.java<br>d/a/a/a/e/b.java<br>com/abbondioendrizzi/antivirus/supercleaner/screen/junkfile/JunkFileActivity.java<br>d/o/a/k/a.java<br>d/a/a/a/d/k.java<br>com/testapp/duplicatefileremover/MainActivity.java<br>org/litepal/LitePal.java<br>d/a/a/a/j/t.java<br>org/litepal/tablemanager/Connector.java |
| 6 | The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks. | high | CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-3 | d/m/a/j/e.java |
| 7 | This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel. | secure | OWASP MASVS: MSTG-NETWORK-4 | h/l0/k/g.java<br>h/l0/k/d.java<br>h/l0/k/c.java<br>h/l0/k/h.java |
| 8 | 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 | b/u/i.java |
| 9 | 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 | d/d/a/m/u/q.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 10 | SHA-1 is a weak hash known to have hash collisions. | warning | CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | d/a/a/a/g/g/b.java |

# NIAP ANALYSIS v1.3

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|
| 1 | FCS_RBG_EXT.1.1 | Security Functional Requirements | Random Bit Generation Services | The application use no DRBG functionality for its cryptographic operations. |
| 2 | FCS_STO_EXT.1.1 | Security Functional Requirements | Storage of Credentials | The application does not store any credentials to non-volatile memory. |
| 3 | FCS_CKM_EXT.1.1 | Security Functional Requirements | Cryptographic Key Generation Services | The application generate no asymmetric cryptographic keys. |
| 4 | FDP_DEC_EXT.1.1 | Security Functional Requirements | Access to Platform Resources | The application has access to ['network connectivity', 'bluetooth', 'camera']. |
| 5 | FDP_DEC_EXT.1.2 | Security Functional Requirements | Access to Platform Resources | The application has access to no sensitive information repositories. |
| 6 | FDP_NET_EXT.1.1 | Security Functional Requirements | Network Communications | The application has user/application initiated network communications. |

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|
| 7 | FDP_DAR_EXT.1.1 | Security Functional Requirements | Encryption Of Sensitive Application Data | The application implement functionality to encrypt sensitive data in non-volatile memory. |
| 8 | FMT_MEC_EXT.1.1 | Security Functional Requirements | Supported Configuration Mechanism | The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options. |
| 9 | FTP_DIT_EXT.1.1 | Security Functional Requirements | Protection of Data in Transit | The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product. |
| 10 | FCS_COP.1.1(1) | Selection-Based Security Functional Requirements | Cryptographic Operation - Encryption/Decryption | The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit. |
| 11 | FCS_COP.1.1(2) | Selection-Based Security Functional Requirements | Cryptographic Operation - Hashing | The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5. |
| 12 | FCS_HTTPS_EXT.1.2 | Selection-Based Security Functional Requirements | HTTPS Protocol | The application implement HTTPS using TLS. |
| 13 | FCS_HTTPS_EXT.1.3 | Selection-Based Security Functional Requirements | HTTPS Protocol | The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid. |
| 14 | FIA_X509_EXT.2.1 | Selection-Based Security Functional Requirements | X.509 Certificate Authentication | The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS. |

# DOMAIN MALWARE CHECK

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| statscodicefiscale.xyz | malware<br>**URL:** statscodicefiscale.xyz **IP:** N/A **Description:** Malicious Domain tagged by Maltrail | **IP:** 176.10.119.156<br>**Country:** Switzerland<br>**Region:** Zug<br>**City:** Hunenberg<br>**Latitude:** 47.175362<br>**Longitude:** 8.424970<br>**View:** Google Map |
| ns.adobe.com | ok | No Geolocation information available. |
| github.com | ok | **IP:** 140.82.121.4<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 |
| play.google.com | ok | **IP:** 142.251.36.46<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 |
| linkyourpage.com | ok | No Geolocation information available. |

# EMAILS

| EMAIL | FILE |
| --- | --- |
| android.studio@android.com | Android String Resource |

# HARDCODED SECRETS

| POSSIBLE SECRETS |
| --- |
| "library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1" |

---

## Report Generated by - MobSF v3.5.2 Beta

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

© 2022 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.