# ANDROID STATIC ANALYSIS REPORT

app_icon

## GPS (1.0)

| | |
|---|---|
| File Name: | app-debug.apk |
| Package Name: | gpskill.gps |
| Scan Date: | Oct. 24, 2024, 7:59 p.m. |
| App Security Score: | 36/100 (HIGH RISK) |
| Grade: | C |

# FINDINGS SEVERITY

| HIGH | MEDIUM | INFO | SECURE | HOTSPOT |
|---|---|---|---|---|
| 3 | 2 | 0 | 1 | 1 |

# FILE INFORMATION

**File Name:** app-debug.apk
**Size:** 6.18MB
**MD5:** 53e36efc77a29d1db735cd827c171cab
**SHA1:** 40a69b83d7be04861596a768b3451f5c88e887b8
**SHA256:** 7f5b1e6987816c69542158783ca1de7831ca9c8277674759c20c7a43dd22741a

# APP INFORMATION

**App Name:** GPS
**Package Name:** gpskill.gps
**Main Activity:** gpskill.gps.MainActivity
**Target SDK:** 34
**Min SDK:** 24
**Max SDK:**
**Android Version Name:** 1.0
**Android Version Code:** 1

# APP COMPONENTS

**Activities:** 3
**Services:** 0
**Receivers:** 1
**Providers:** 1
**Exported Activities:** 0
**Exported Services:** 0
**Exported Receivers:** 1
**Exported Providers:** 0

# CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=Android Debug, O=Android, C=US
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-08-29 20:24:03+00:00
Valid To: 2054-08-22 20:24:03+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha256
md5: 7bc90405f1aae86733193e9a0e590e99
sha1: 4c347a2cac305c8fb02a9acbb6c75669bb378dd6
sha256: a4058cac632cc28e66d09ca61bbed66abba3e676a7fea776ed9430f4e1c0228e
sha512: 0c17f397ee1e2388460d0e9990b096e772faa5e88f814595f18f832160f23781d0d93e48a3c255c14964d3c4d32327959fc5663f13086dc1a4ee2b71e31e5167
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 968b935229868c130a529c925db8bb6ef5b1047f85b86fde79c3675e3ff8ba11
Found 1 unique certificates

# APPLICATION PERMISSIONS

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| 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.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_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. |
| android.permission.INTERNET | normal | full Internet access | Allows an application to create network sockets. |
| gpskill.gps.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION | unknown | Unknown permission | Unknown permission from android reference |

# APKID ANALYSIS

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

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

| 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.BRAND check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table> |

# NETWORK SECURITY

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

# CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

| TITLE | SEVERITY | DESCRIPTION |
|---|---|---|
| Signed Application | info | Application is signed with a code signing certificate |
| Application signed with debug certificate | high | Application signed with a debug certificate. Production application must not be shipped with a debug certificate. |

# MANIFEST ANALYSIS

HIGH: 2 | WARNING: 2 | INFO: 0 | SUPPRESSED: 0

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 1 | App can be installed on a vulnerable upatched 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 | Debug Enabled For App<br>[android:debuggable=true] | high | Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes. |
| 3 | Application Data can be Backed up<br>[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. |
| 4 | 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

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|

# NIAP ANALYSIS v1.3

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

# ABUSED PERMISSIONS

| TYPE | MATCHES | PERMISSIONS |
|---|---|---|
| Malware Permissions | 4/24 | android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET |
| Other Common Permissions | 0/45 | |

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

# SCAN LOGS

| Timestamp | Event | Error |
|---|---|---|
| 2024-10-24 20:05:11 | Generating Hashes | OK |

| | | |
|---|---|---|
| 2024-10-24 20:05:12 | Extracting APK | OK |
| 2024-10-24 20:05:12 | Unzipping | OK |
| 2024-10-24 20:05:13 | Getting Hardcoded Certificates/Keystores | OK |
| 2024-10-24 20:05:13 | Parsing AndroidManifest.xml | OK |
| 2024-10-24 20:05:13 | Parsing APK with androguard | OK |
| 2024-10-24 20:05:17 | Extracting Manifest Data | OK |
| 2024-10-24 20:05:17 | Performing Static Analysis on: GPS (gpskill.gps) | OK |
| 2024-10-24 20:05:17 | Fetching Details from Play Store: gpskill.gps | OK |
| 2024-10-24 20:05:17 | Detecting Trackers | OK |
| 2024-10-24 20:05:18 | Manifest Analysis Started | OK |

| | | |
|---|---|---|
| 2024-10-24 20:05:18 | Checking for Malware Permissions | OK |
| 2024-10-24 20:05:18 | Fetching icon path | OK |
| 2024-10-24 20:05:18 | Library Binary Analysis Started | OK |
| 2024-10-24 20:05:19 | Reading Code Signing Certificate | OK |
| 2024-10-24 20:05:20 | Detecting Trackers | OK |
| 2024-10-24 20:05:22 | Running APKiD 2.1.5 | OK |
| 2024-10-24 20:05:35 | Converting DEX to Smali | OK |
| 2024-10-24 20:05:35 | Code Analysis Started on - java_source | OK |
| 2024-10-24 20:05:36 | Detecting Trackers | OK |
| 2024-10-24 20:05:39 | Decompiling APK to Java with jadx | OK |
| 2024-10-24 20:05:43 | libsast scan failed | FileNotFoundError(2, 'No such file or directory') |

| | | |
|---|---|---|
| 2024-10-24 20:05:43 | Android SAST Completed | OK |
| 2024-10-24 20:05:43 | Android API Analysis Started | OK |
| 2024-10-24 20:05:52 | Decompiling APK to Java with jadx | OK |
| 2024-10-24 20:05:53 | Android Permission Mapping Started | OK |
| 2024-10-24 20:05:56 | Android Permission Mapping Completed | OK |
| 2024-10-24 20:05:56 | Finished Code Analysis, Email and URL Extraction | OK |
| 2024-10-24 20:05:56 | Extracting String data from APK | OK |
| 2024-10-24 20:06:00 | Extracting String data from Code | OK |
| 2024-10-24 20:06:00 | Extracting String values and entropies from Code | OK |
| 2024-10-24 20:06:01 | Performing Malware check on extracted domains | OK |
| 2024-10-24 20:06:02 | Saving to Database | OK |

| | | |
|---|---|---|
| 2024-10-24 20:06:15 | Decompiling APK to Java with jadx | OK |
| 2024-10-24 20:06:57 | Converting DEX to Smali | OK |
| 2024-10-24 20:06:57 | Code Analysis Started on - java_source | OK |
| 2024-10-24 20:10:20 | Converting DEX to Smali | OK |
| 2024-10-24 20:10:21 | Code Analysis Started on - java_source | OK |
| 2024-10-24 20:11:33 | Converting DEX to Smali | OK |
| 2024-10-24 20:11:33 | Code Analysis Started on - java_source | OK |

---

## Report Generated by - MobSF v4.0.7

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.