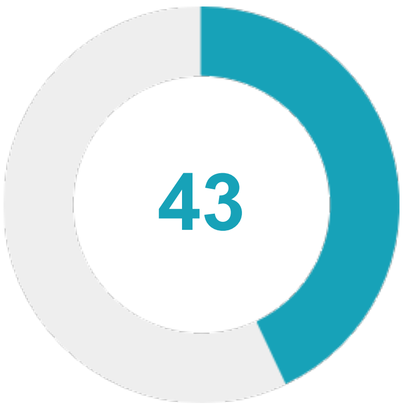
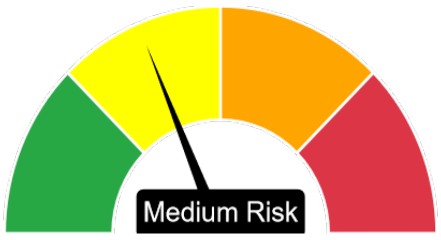
☆ Security Score



Security Score 43/100

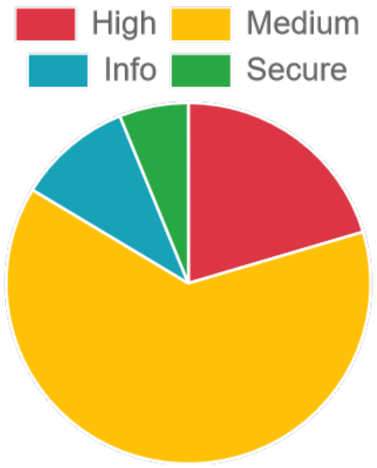
Risk Rating



Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

5

User/Device Trackers

Findings

High **6**

Medium **18**

Info **3**

Secure **2**

Hotspot **1**

high Certificate algorithm vulnerable to hash collision — CERTIFICATE

high Clear text traffic is Enabled For App — MANIFEST

high The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks. — CODE

high The file or SharedPreference is World Writable. Any App can write to the file — CODE

high The file or SharedPreference is World Readable. Any App can read from the file — CODE

high Application contains Privacy Trackers — TRACKERS

medium App can be installed on a vulnerable Android version — MANIFEST

medium Broadcast Receiver (com.appsflyer.MultipleInstallBroadcastReceiver) is not Protected. — MANIFEST

medium TaskAffinity is set for activity — MANIFEST

medium Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. — MANIFEST

medium Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. — MANIFEST

medium Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. — MANIFEST

medium Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. — MANIFEST

CODE

medium App creates temp file. Sensitive information should never be written into a temp file.

medium Files may contain hardcoded sensitive information like usernames, passwords, keys etc. CODE

medium 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. CODE

medium App can read/write to External Storage. Any App can read data written to External Storage. CODE

medium The App uses an insecure Random Number Generator. CODE

medium MD5 is a weak hash known to have hash collisions. CODE

medium SHA-1 is a weak hash known to have hash collisions. CODE

medium Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole. CODE

medium Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system. CODE

medium This App may request root (Super User) privileges. CODE

medium This app may contain hardcoded secrets SECRETS

info The App logs information. Sensitive information should never be logged. CODE

info App can write to App Directory. Sensitive Information should be encrypted. CODE

info This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it. CODE

secure This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel. CODE

secure This App may have root detection capabilities. CODE

hotspot Found 18 critical permission(s) PERMISSIONS

MobSF Application Security Scorecard generated for No icon (Life360 24.29.0)

Version v4.0.6