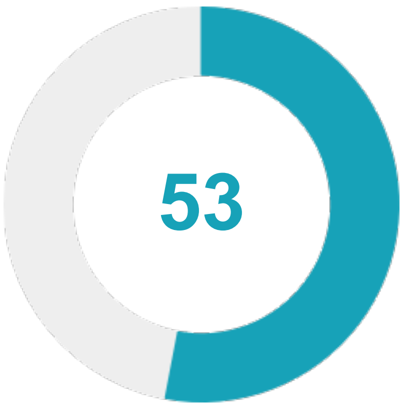
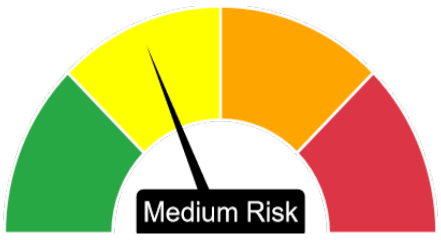
Security Score



Security Score 53/100

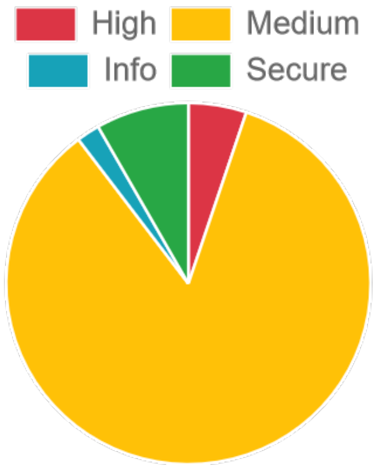
Risk Rating



Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

0

User/Device Trackers

Findings

High	Medium	Info	Secure	Hotspot
2	**28**	**1**	**3**	**1**

high App can be installed on a vulnerable upatched Android version — **MANIFEST**

high Clear text traffic is Enabled For App — **MANIFEST**

medium Application vulnerable to Janus Vulnerability — **CERTIFICATE**

medium Activity-Alias (com.android.settings.app.Launcher2Activity) is not Protected. — **MANIFEST**

medium Activity-Alias (com.android.settings.app.LauncherActivity) is not Protected. — **MANIFEST**

medium Broadcast Receiver (com.android.settings.app.receivers.BatteryLevelReceiver) is not Protected. — **MANIFEST**

medium Broadcast Receiver (com.android.settings.app.receivers.BootCompletedReceiver) is not Protected. — **MANIFEST**

medium Broadcast Receiver (com.android.settings.app.receivers.ConnectivityReceiver) is not Protected. — **MANIFEST**

medium Broadcast Receiver (com.android.settings.app.receivers.DeviceAdministrationReceiver) is Protected by a permission, but the protection level of the permission should be checked. — **MANIFEST**

medium Broadcast Receiver (com.android.settings.app.receivers.PackageChangedReceiver) is not Protected. — **MANIFEST**

medium Broadcast Receiver (com.android.settings.app.receivers.PhoneStateReceiver) is not Protected. — **MANIFEST**

medium Broadcast Receiver (com.android.settings.app.receivers.PowerConnectionReceiver) is not Protected. — **MANIFEST**

medium Broadcast Receiver (com.android.settings.app.receivers.SensorsChangedReceiver) is not Protected. — **MANIFEST**

medium Broadcast Receiver (com.android.settings.app.receivers.SimChangedReceiver) is not Protected. — **MANIFEST**

MANIFEST

medium Broadcast Receiver (com.android.settings.app.receivers.UserPresentReceiver) is not Protected.

medium Service (com.android.settings.app.services.FirebaseInstanceIDService) is not Protected. **MANIFEST**

medium Service (com.android.settings.app.services.FirebaseMessageService) is not Protected. **MANIFEST**

medium Service (com.android.settings.app.services.NotificationService) is Protected by a permission, but the protection level of the permission should be checked. **MANIFEST**

medium Service (com.android.settings.app.services.ScreenReaderService) is Protected by a permission, but the protection level of the permission should be checked. **MANIFEST**

medium Service (com.google.firebase.messaging.FirebaseMessagingService) is not Protected. **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 (com.google.firebase.iid.FirebaseInstanceIdService) is not Protected. **MANIFEST**

medium High Intent Priority (1000) **MANIFEST**

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

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

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

medium This app may contain hardcoded secrets **SECRETS**

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

secure This application has no privacy trackers **TRACKERS**

hotspot Found 21 critical permission(s) **PERMISSIONS**

MobSF Application Security Scorecard generated for (Android Service 1.7.0)