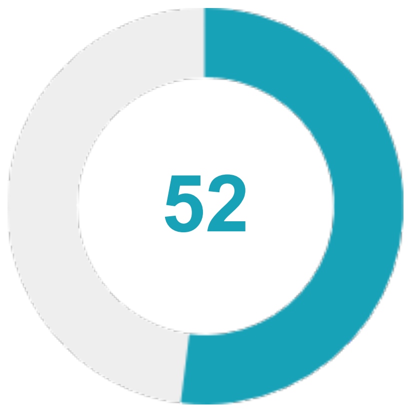
Security Score



Security Score 52/100

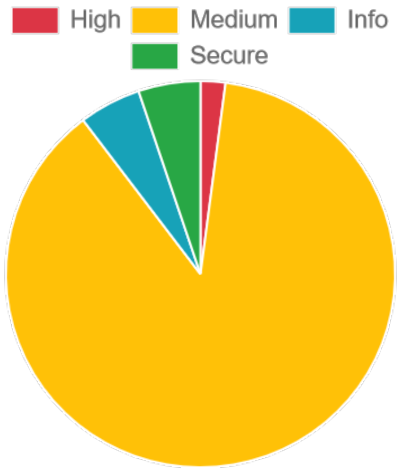
Risk Rating

Medium Risk

Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

3

User/Device Trackers

Findings

High	**1**
Medium	**30**
Info	**2**
Secure	**2**
Hotspot	**1**

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

medium Application Data can be Backed up **MANIFEST**

medium Service (io.familytime.parentalcontrol.fcm.MyFirebaseMessagingService) is not Protected. **MANIFEST**

medium Service (io.familytime.parentalcontrol.services.AccessibilityService) is Protected by a permission, but the protection level of the permission should be checked. **MANIFEST**

medium Service (io.familytime.parentalcontrol.services.AccessibilityService) is Protected by a permission, but the protection level of the permission should be checked. **MANIFEST**

medium Broadcast Receiver (io.familytime.parentalcontrol.featuresList.battery.BatteryStatusReceiver) is not Protected. **MANIFEST**

medium Broadcast Receiver (io.familytime.parentalcontrol.featuresList.location.LocationUpdateReceiver) is not Protected. **MANIFEST**

medium Broadcast Receiver (io.familytime.parentalcontrol.featuresList.location.LocationUpdatesBroadcastReceiver) is not Protected. **MANIFEST**

medium Broadcast Receiver (io.familytime.parentalcontrol.receivers.DateTimeChangeReceiver) is not Protected. **MANIFEST**

medium Broadcast Receiver (io.familytime.parentalcontrol.receivers.MyDeviceAdminReceiver) is Protected by a permission, but the protection level of the permission should be checked. **MANIFEST**

medium Broadcast Receiver (io.familytime.parentalcontrol.featuresList.installAppModule.receivers.AppInstallReceiver) is not Protected. **MANIFEST**

medium Broadcast Receiver (io.familytime.parentalcontrol.featuresList.installAppModule.receivers.InstallAppsUploadReceiver) is not Protected. **MANIFEST**

medium Broadcast Receiver (io.familytime.parentalcontrol.featuresList.smsmodule.reciever.SmsBroadcastReceiver) is not **MANIFEST**

Protected.

medium Broadcast Receiver (io.familytime.parentalcontrol.featuresList.contactWatchList.ContactsWatchlistReceiver) is not Protected. MANIFEST

medium Broadcast Receiver (io.familytime.parentalcontrol.receivers.AppReceiver) is not Protected. MANIFEST

medium Broadcast Receiver (io.familytime.parentalcontrol.featuresList.geofence.GeofenceBroadcastReceiver) is not Protected. MANIFEST

medium Service (io.familytime.parentalcontrol.featuresList.notificationLisner.NotificationService) is Protected by a permission, but the protection level of the permission should be checked. 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

medium High Intent Priority (999) MANIFEST

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

medium The App uses an insecure Random Number Generator. CODE

medium IP Address disclosure CODE

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

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

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

medium Application contains Privacy Trackers TRACKERS

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

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 13 critical permission(s) PERMISSIONS

MobSF Application Security Scorecard generated for No icon (FamilyTime Jr 3.14.6.ps)