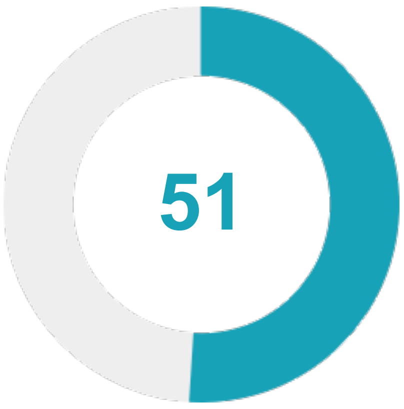
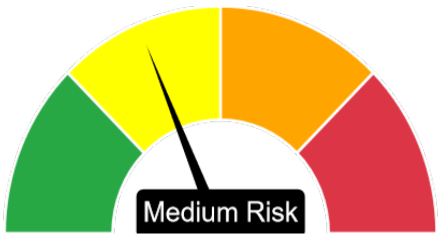
Security Score



Security Score 51/100

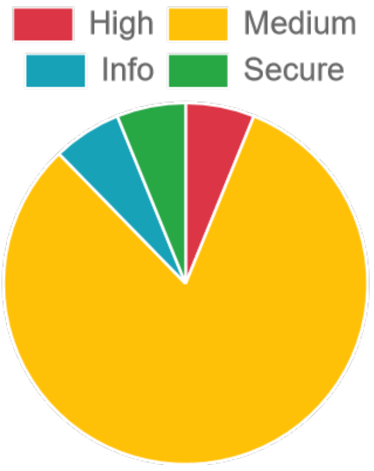
Risk Rating



Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

4

User/Device Trackers

Findings

High	Medium	Info	Secure	Hotspot
2	24	2	2	1

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

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

medium Activity (app.kids360.kid.ui.main.MainActivity) is not Protected. — MANIFEST

medium Broadcast Receiver (app.kids360.usages.read.ShutdownRegistrator) is Protected by a permission, but the protection level of the permission should be checked. — MANIFEST

medium Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.SleepEventReceiver) is Protected by a permission, but the protection level of the permission should be checked. — MANIFEST

medium Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.BootReceiver) is Protected by a permission, but the protection level of the permission should be checked. — MANIFEST

medium Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.PassiveReceiver) is not Protected. — MANIFEST

medium Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.ActivityReceiver) is not Protected. — MANIFEST

medium Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.PassiveFusedReceiver) is not Protected. — MANIFEST

medium Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.StationReceiver) is not Protected. — MANIFEST

medium Broadcast Receiver (org.findmykids.geo.producer.presentation.receiver.ActivityEventReceiver) is Protected by a permission, but the protection level of the permission should be checked. — MANIFEST

medium Service (org.findmykids.geo.producer.presentation.service.BootJobSchedulerService) 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 (com.google.firebase.iid.FirebaseInstanceIdReceiver) 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 The App uses an insecure Random Number Generator. CODE

medium Files may contain hardcoded sensitive information like usernames, passwords, keys etc. 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 Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole. CODE

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

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

medium IP Address disclosure 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 This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it. CODE

secure This App may have root detection capabilities. CODE

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

hotspot Found 10 critical permission(s) PERMISSIONS

MobSF Application Security Scorecard generated for (Alli360 2.17.0)