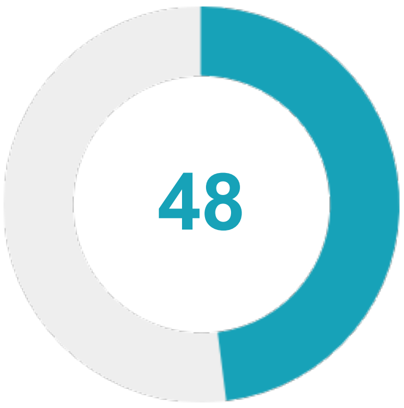
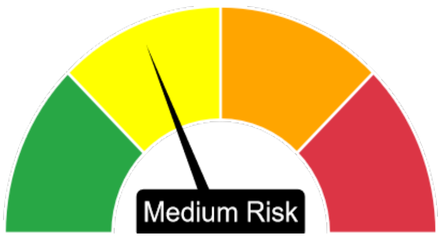
Security Score



Security Score 48/100

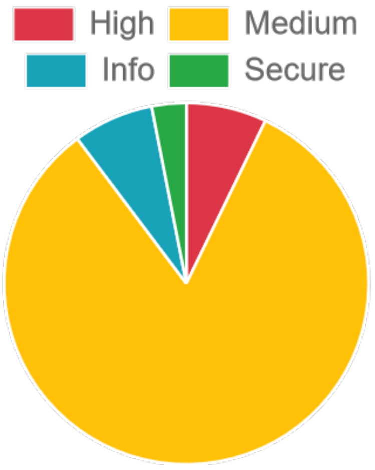
Risk Rating



Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

3

User/Device Trackers

Findings

High
2

Medium
22

Info
2

Secure
1

Hotspot
2

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 Certificate algorithm might be vulnerable to hash collision CERTIFICATE

medium Service (com.qustodio.qustodioapp.service.messaging.FirebaseMessagingService) is not Protected. MANIFEST

medium Activity (com.qustodio.qustodioapp.ui.onboarding.chromeextension.setup.ChromeExtensionSetupActivity) is not Protected. MANIFEST

medium Activity (com.qustodio.qustodioapp.ui.passwordrequest.login.LoginPasswordRequestActivity) is not Protected. MANIFEST

medium Service (com.qustodio.qustodioapp.service.RestartServiceNotification) is Protected by a permission, but the protection level of the permission should be checked. MANIFEST

medium Service (com.qustodio.qustodioapp.accessibility.AccessibilityService) 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

MANIFEST

medium High Intent Priority (999)

MANIFEST

medium High Intent Priority (998)

MANIFEST

medium High Intent Priority (2147483647)

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

CODE

medium IP Address disclosure

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.

TRACKERS

medium Application contains Privacy Trackers

SECRETS

medium This app may contain hardcoded secrets

CODE

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.

PERMISSIONS

hotspot Found 5 critical permission(s)

FILES

hotspot Found 1 certificate/key file(s)

MobSF Application Security Scorecard generated for (Qustodio Kids 180.70.1.2-family)

Version v4.0.6