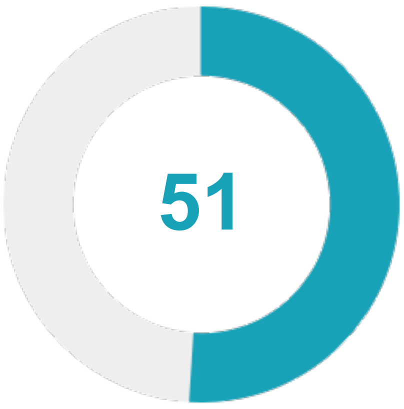
Security Score



Security Score 51/100

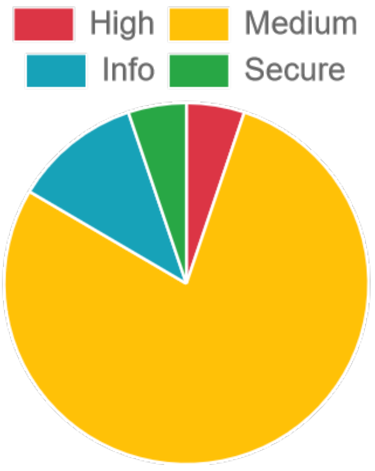
Risk Rating

Medium Risk

Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

1

User/Device Trackers

Findings

High	Medium	Info	Secure	Hotspot
1	**13**	**2**	**1**	**1**

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

medium Application Data can be Backed up — MANIFEST

medium Activity (com.canhub.cropper.CropImageActivity) is not Protected. — MANIFEST

medium Broadcast Receiver (kz.sirius.siriuschat.applimits.AppInstallReceiver) 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 (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 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 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 App creates temp file. Sensitive information should never be written into a temp file. — CODE

medium Application contains Privacy Trackers — TRACKERS

SECRETS

medium This app may contain hardcoded 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

hotspot Found 12 critical permission(s) PERMISSIONS

MobSF Application Security Scorecard generated for (1Tigrow 1.345)