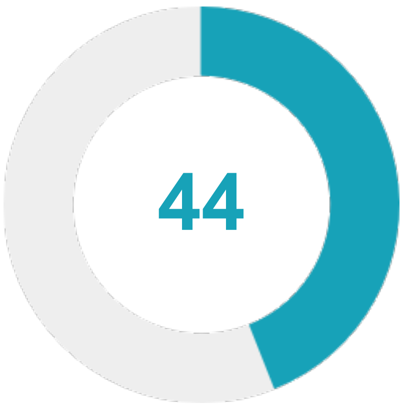
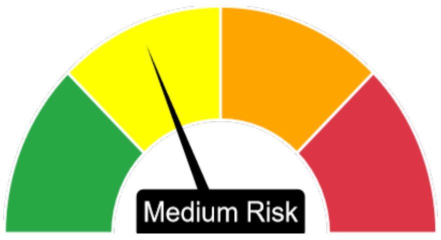
Security Score



Security Score 44/100

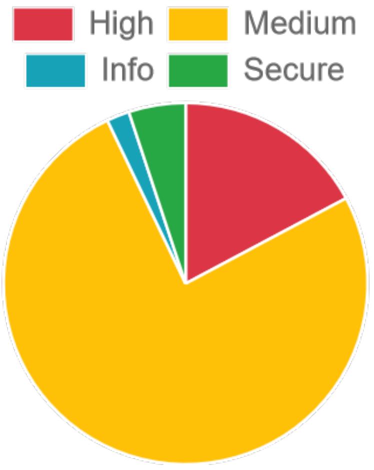
Risk Rating



Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

4

User/Device Trackers

Findings

High	Medium	Info	Secure	Hotspot
7	**30**	**1**	**2**	**1**

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

high Clear text traffic is Enabled For App — MANIFEST

high Activity (com.play.services.PLACEHOLDER) is vulnerable to StrandHogg 2.0 — MANIFEST

high Activity (com.play.services.PRODUCT) is vulnerable to StrandHogg 2.0 — MANIFEST

high Activity (c.a.b.core.ui.activity.KeepAliveServiceStartActivity) is vulnerable to StrandHogg 2.0 — MANIFEST

high Activity (com.google.firebase.auth.internal.GenericIdpActivity) is vulnerable to StrandHogg 2.0 — MANIFEST

high Activity (com.google.firebase.auth.internal.RecaptchaActivity) is vulnerable to StrandHogg 2.0 — MANIFEST

medium Application vulnerable to Janus Vulnerability — CERTIFICATE

medium Activity-Alias (com.play.services.PLACEHOLDER) is not Protected. — MANIFEST

medium Activity-Alias (com.play.services.PRODUCT) is not Protected. — MANIFEST

medium Activity (c.a.b.core.ui.activity.KeepAliveServiceStartActivity) is not Protected. — MANIFEST

medium Broadcast Receiver (c.a.b.app.receiver.MainReceiver) is not Protected. — MANIFEST

medium Broadcast Receiver (c.a.b.app.receiver.ForceReceiver) is not Protected. — MANIFEST

medium Broadcast Receiver (c.a.b.app.receiver.AdminReceiver) is Protected by a permission, but the protection level of the permission should be checked. — MANIFEST

MANIFEST

medium Service (c.a.b.core.service.AccessibilityService) is Protected by a permission, but the protection level of the permission should be checked.

MANIFEST

medium Service (c.a.b.core.service.KeepAliveJobService) is Protected by a permission, but the protection level of the permission should be checked.

MANIFEST

medium Service (c.a.b.core.service.KeepAliveLocalService) is not Protected.

MANIFEST

medium Service (c.a.b.core.service.KeepAliveRemoteService) is not Protected.

MANIFEST

medium Service (c.a.b.auth.service.AuthenticationService) is not Protected.

MANIFEST

medium Service (c.a.b.auth.service.SyncAccountService) is not Protected.

MANIFEST

medium Broadcast Receiver (c.a.b.lock.receiver.SmsReceiver) is Protected by a permission, but the protection level of the permission should be checked.

MANIFEST

medium Broadcast Receiver (c.a.b.lock.receiver.MmsReceiver) is Protected by a permission, but the protection level of the permission should be checked.

MANIFEST

medium Activity (c.a.b.lock.ui.activity.ComposeSmsActivity) is not Protected.

MANIFEST

medium Service (c.a.b.lock.service.HeadlessSmsSendService) 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 Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected.

MANIFEST

medium Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected.

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

CODE

medium IP Address disclosure

CODE

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

CODE

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.

TRACKERS

medium Application contains Privacy Trackers 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

hotspot Found 28 critical permission(s) PERMISSIONS

MobSF Application Security Scorecard generated for (Play services 3.11.3)