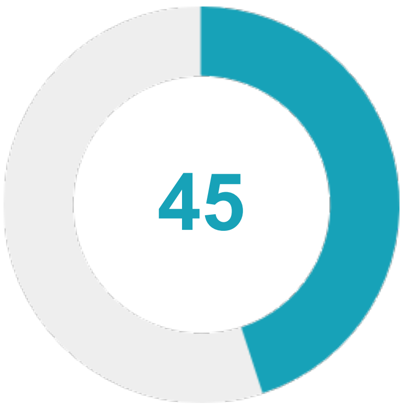
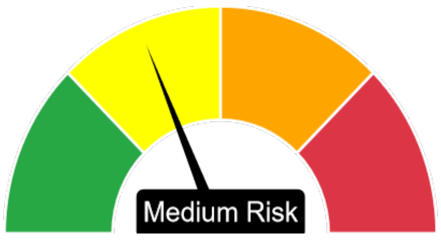
Security Score



Security Score 45/100

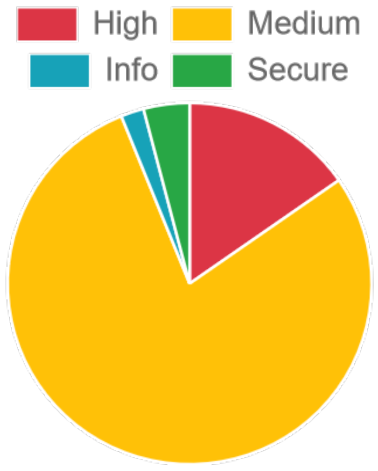
Risk Rating



Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

5

User/Device Trackers

Findings

High	**7**
Medium	**35**
Info	**1**
Secure	**2**
Hotspot	**2**

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

high Debug Enabled For App — MANIFEST

high Activity (com.google.android.gms.appinvite.PreviewActivity) is vulnerable to StrandHogg 2.0 — MANIFEST

high Activity (com.google.android.gms.tagmanager.TagManagerPreviewActivity) is vulnerable to StrandHogg 2.0 — MANIFEST

high Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks — CODE

high Debug configuration enabled. Production builds must not be debuggable. — CODE

high Application contains Privacy Trackers — TRACKERS

medium Application vulnerable to Janus Vulnerability — CERTIFICATE

medium Activity (com.system.task.ui.LockScreen) is not Protected. — MANIFEST

medium Service (com.system.task.services.ZTIService) is not Protected. — MANIFEST

medium Service (com.system.task.services.MyFirebaseMessagingService) is not Protected. — MANIFEST

medium Service (com.system.task.services.MyFirebaseInstanceIDService) is not Protected. — MANIFEST

medium Broadcast Receiver (com.system.task.receivers.AndroidBroadcastReceiver) is not Protected. — MANIFEST

medium Broadcast Receiver (com.system.task.receivers.ServiceAlarmReceiver) is not Protected. — MANIFEST

MANIFEST

medium	Broadcast Receiver (com.system.task.receivers.AndroidTelephonyReceiver) is not Protected.	
medium	Broadcast Receiver (com.system.task.receivers.AndroidScreenOnOffReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.system.task.receivers.EnterpriseDeviceAdminReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Broadcast Receiver (com.system.task.receivers.PackageChangeReceiver) is not Protected.	MANIFEST
medium	Service (com.system.task.accessibility.SystemAccessibilityService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Activity (com.system.task.ui.CustomActivity) is not Protected.	MANIFEST
medium	Service (com.system.task.services.ScreenShotNonRootedService) is not Protected.	MANIFEST
medium	Service (com.system.task.services.NotificationService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Activity (com.google.android.gms.appinvite.PreviewActivity) is not Protected.	MANIFEST
medium	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Launch Mode of activity (com.google.firebase.auth.internal.FederatedSignInActivity) is not standard.	MANIFEST
medium	Activity (com.google.firebase.auth.internal.FederatedSignInActivity) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Activity (com.google.android.gms.tagmanager.TagManagerPreviewActivity) is not Protected.	MANIFEST
medium	Service (com.google.firebase.messaging.FirebaseMessagingService) is not Protected.	MANIFEST
medium	Service (com.firebase.jobdispatcher.GooglePlayReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) 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 (com.google.firebase.iid.FirebaseInstanceIdService) is not Protected.	MANIFEST
medium	High Intent Priority (999)	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 App can read/write to External Storage. Any App can read data written to External Storage. CODE

medium The App uses an insecure Random Number Generator. 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 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 18 critical permission(s) PERMISSIONS

hotspot Found 1 certificate/key file(s) FILES

MobSF Application Security Scorecard generated for (Android Auto 6.5)

© 2024 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.