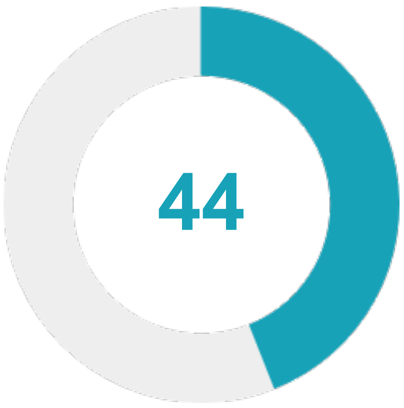
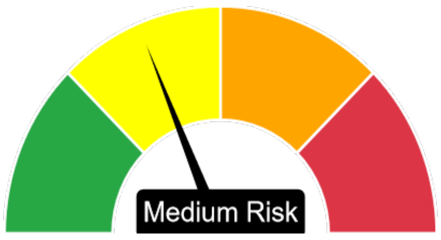
Security Score



Security Score 44/100

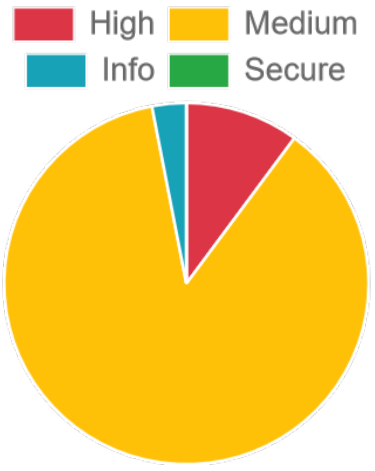
Risk Rating



Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

1

User/Device Trackers

Findings

High **3**	Medium **26**	Info **1**	Secure **0**	Hotspot **1**

high	App can be installed on a vulnerable upatched Android version	MANIFEST
high	Weak Encryption algorithm used	CODE
high	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	CODE
medium	Application vulnerable to Janus Vulnerability	CERTIFICATE
medium	Service (com.fp.CoreService) is not Protected.	MANIFEST
medium	Service (com.fp.spy_call.service.SpyService) is not Protected.	MANIFEST
medium	Service (com.fp.WDService) is not Protected.	MANIFEST
medium	Service (com.fp.capture.appscreenshot.ProjectionService) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.fp.receiver.CommonReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.fp.callhandler.phonestate.OutgoingCallReceiver) is not Protected.	MANIFEST
medium	Service (com.fp.accessibilityservice.NMAccessibilityService) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Broadcast Receiver (com.fp.receiver.AppDeviceAdminReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (com.fp.google_push_notification_manager.MyFirebaseInstanceIDService) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.fp.google_push_notification_manager.FirebaseDataReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST

medium Service (com.fp.capture.callrecorder.accessibility_use.VoIPCallRecordingStateNotifier) 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 (2147483647) MANIFEST

medium High Intent Priority (2147483647) 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 SHA-1 is a weak hash known to have hash collisions. 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 The App uses an insecure Random Number Generator. CODE

medium Files may contain hardcoded sensitive information like usernames, passwords, keys etc. CODE

medium This App may request root (Super User) privileges. 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

hotspot Found 24 critical permission(s) PERMISSIONS

MobSF Application Security Scorecard generated for (Sync Services 5.3.3)