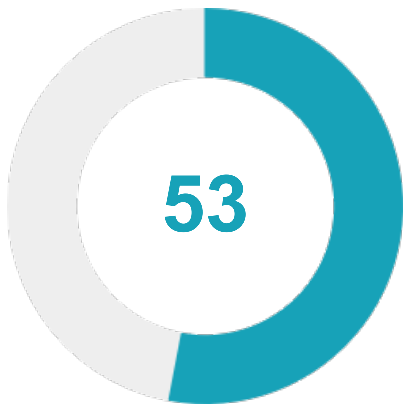
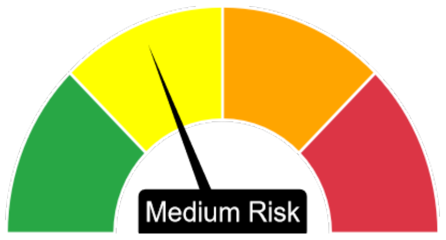
Security Score



Security Score 53/100

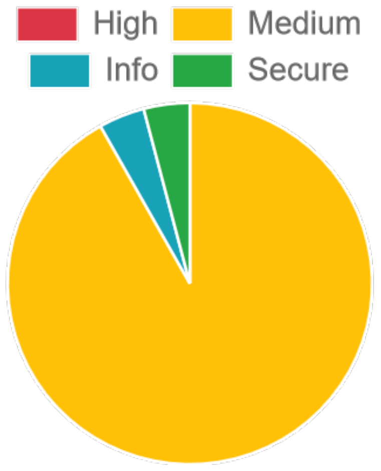
Risk Rating



Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

3

User/Device Trackers

Findings

High	**0**
Medium	**37**
Info	**2**
Secure	**2**
Hotspot	**1**

medium Base config is configured to trust system certificates **NETWORK**

medium App can be installed on a vulnerable Android version **MANIFEST**

medium TaskAffinity is set for activity **MANIFEST**

medium Service (com.microsoft.familysafety.screentime.services.FamilySafetyAccessibilityService) is Protected by a permission, but the protection level of the permission should be checked. **MANIFEST**

medium Service (com.microsoft.familysafety.core.pushnotification.FirebaseCloudMessagingService) is not Protected. **MANIFEST**

medium Broadcast Receiver (com.microsoft.familysafety.core.broadcasts.UninstallAppReceiver) is not Protected. **MANIFEST**

medium Broadcast Receiver (com.microsoft.familysafety.screentime.admin.AdminReceiver) is Protected by a permission, but the protection level of the permission should be checked. **MANIFEST**

medium Activity (com.microsoft.appcenter.distribute.DeepLinkActivity) is not Protected. **MANIFEST**

medium Broadcast Receiver (com.microsoft.appcenter.distribute.DownloadManagerReceiver) is not Protected. **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.sentiance.sdk.BootCompletedReceiver) is not Protected. **MANIFEST**

medium Broadcast Receiver (com.sentiance.sdk.TimezoneChangeReceiver) is not Protected. **MANIFEST**

MANIFEST

medium Broadcast Receiver (com.sentiance.sdk.location.LocationProviderChangeReceiver) is not Protected.

medium Broadcast Receiver (com.sentiance.sdk.DebugReceiver) is not Protected. **MANIFEST**

medium Broadcast Receiver (com.sentiance.sdk.task.ConnectivityChangeReceiver) is not Protected. **MANIFEST**

medium Broadcast Receiver (com.sentiance.sdk.task.PowerStateChangedReceiver) is not Protected. **MANIFEST**

medium Broadcast Receiver (com.sentiance.sdk.deviceinfo.UpgradeBroadcastReceiver) is not Protected. **MANIFEST**

medium Broadcast Receiver (com.sentiance.sdk.activitytransition.ActivityTransitionChangeReceiver) is not Protected. **MANIFEST**

medium Broadcast Receiver (com.sentiance.sdk.movingstate.MovingStateTimeoutReceiver) is not Protected. **MANIFEST**

medium Broadcast Receiver (com.sentiance.sdk.movingstate.StationaryAssistantReceiver) is not Protected. **MANIFEST**

medium Broadcast Receiver (com.sentiance.sdk.autostopdetection.SdkDetectionTimeoutReceiver) is not Protected. **MANIFEST**

medium Broadcast Receiver (com.microsoft.beacon.network.WifiStatusReceiver) is not Protected. **MANIFEST**

medium Broadcast Receiver (com.microsoft.beacon.services.BootReceiver) 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 (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. **MANIFEST**

medium Service (com.evernote.android.job.gcm.PlatformGcmService) 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 App creates temp file. Sensitive information should never be written into a temp file. **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 SHA-1 is a weak hash known to have hash collisions. **CODE**

medium IP Address disclosure **CODE**

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

medium Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole. **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**

secure This App may have root detection capabilities. **CODE**

hotspot Found 8 critical permission(s) **PERMISSIONS**

MobSF Application Security Scorecard generated for (Family Safety 1.26.2.1015)

Version v4.0.6