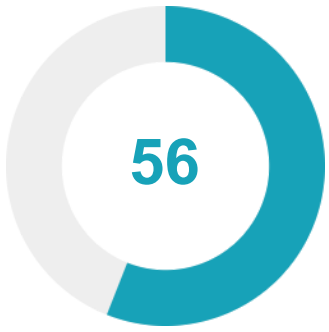
Security Score



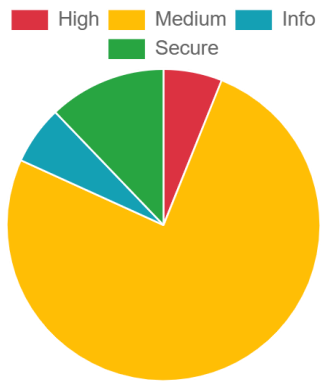
Security Score 56/100

Risk Rating

Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

User/Device Trackers

Findings

High
1

Medium
12

Info
1

Secure
2

Hotspot
2

high The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	CODE
medium Activity (net.openid.appauth.RedirectUriReceiverActivity) 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 Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected.	MANIFEST
medium Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
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 App creates temp file. Sensitive information should never be written into a temp file.	CODE
medium The App uses an insecure Random Number Generator.	CODE
medium IP Address disclosure	CODE
medium SHA-1 is a weak hash known to have hash collisions.	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
secure This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	CODE
secure Firebase Remote Config disabled	FIREBASE
hotspot Found 8 critical permission(s)	PERMISSIONS
hotspot Found 1 certificate/key file(s)	FILES

MobSF Application Security Scorecard generated for (Celcom Digi 1.0.0.11)

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.