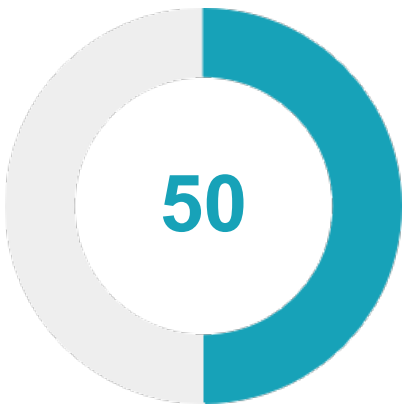
Security Score



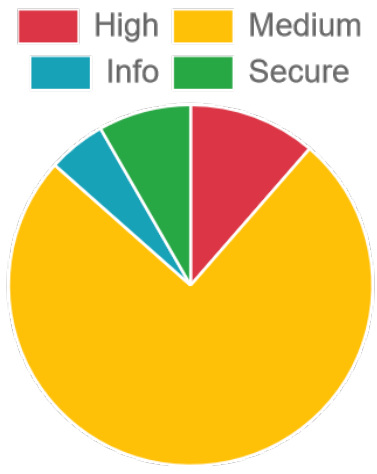
Security Score 50/100

Risk Rating

Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

User/Device Trackers

Findings

High	Medium	Info	Secure	Hotspot
4	25	2	3	2

high App can be installed on a vulnerable upatched Android version	MANIFEST
high The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	CODE
high The file or SharedPreference is World Writable. Any App can write to the file	CODE
high Application contains Privacy Trackers	TRACKERS
medium Certificate algorithm might be vulnerable to hash collision	CERTIFICATE
medium Activity-Alias (com.kaspersky.pctrl.KMSMainLauncher) is not Protected.	MANIFEST
medium Activity (com.kaspersky.pctrl.additional.gui.SchemeActivity) is not Protected.	MANIFEST
medium Activity (com.kaspersky.pctrl.gui.KMSManageSpaceActivity) is not Protected.	MANIFEST
medium Broadcast Receiver (com.kaspersky.pctrl.GcmBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium Broadcast Receiver (com.appsflyer.MultipleInstallBroadcastReceiver) is not Protected.	MANIFEST
medium Service (com.kaspersky.pctrl.rss.KSConnectService) is not Protected.	MANIFEST
medium Service (com.kaspersky.pctrl.messaging.firebase.FcmMessageReceiverService) 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 (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 (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	Service (com.huawei.hms.support.api.push.service.HmsMsgService) is not Protected.	MANIFEST
medium	Content Provider (com.huawei.hms.support.api.push.PushProvider) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.kaspersky.remote.security_service.base.KsUninstallReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	High Intent Priority (999)	MANIFEST
medium	High Intent Priority (999)	MANIFEST
medium	IP Address disclosure	CODE
medium	App can read/write to External Storage. Any App can read data written to External Storage.	CODE
medium	SHA-1 is a weak hash known to have hash collisions.	CODE
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	MD5 is a weak hash known to have hash collisions.	CODE
medium	The App uses an insecure Random Number Generator.	CODE
medium	This app may contain hardcoded secrets	SECRETS
info	The App logs information. Sensitive information should never be logged.	CODE
info	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	CODE
secure	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	CODE
secure	This app has capabilities to prevent tapjacking attacks.	CODE
secure	This App uses SafetyNet API.	CODE
hotspot	Found 8 critical permission(s)	PERMISSIONS
hotspot	Found 1 certificate/key file(s)	FILES

MobSF Application Security Scorecard generated for  (Kaspersky Safe Kids 1.105.0.5)