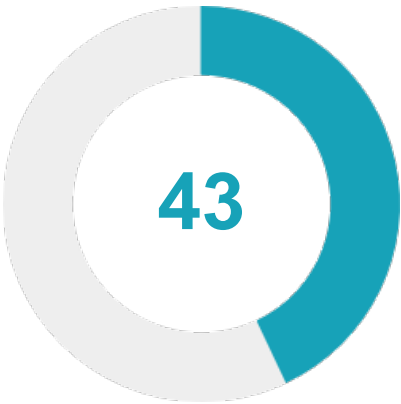


★ Security Score



Security Score 43/100

🚨 Risk Rating

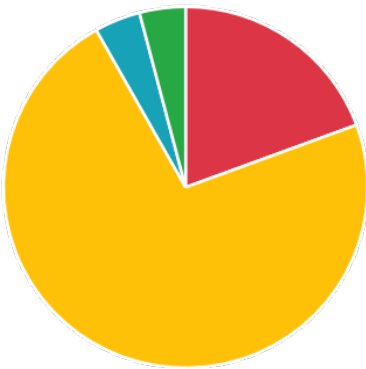


Grade



📊 Severity Distribution (%)

High Medium
Info Secure



👤 Privacy Risk



User/Device Trackers

📄 Findings



High
8



Medium
30



Info
2



Secure
2



Hotspot
3

high App can be installed on a vulnerable upatched Android version

[MANIFEST](#)

high Clear text traffic is Enabled For App

[MANIFEST](#)

high Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks

[CODE](#)

high Remote WebView debugging is enabled.

[CODE](#)

high The file or SharedPreferences is World Writable. Any App can write to the file

[CODE](#)

high The file or SharedPreferences is World Readable. Any App can read from the file

[CODE](#)

high The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.

[CODE](#)

high Application contains Privacy Trackers

[TRACKERS](#)

medium Activity (com.wondershare.famisafe.kids.activity.AllowActivity) is not Protected.

[MANIFEST](#)

medium Activity (com.sensorsdata.analytics.android.sdk.dialog.SchemeActivity) is not Protected.

[MANIFEST](#)

medium Service (com.wondershare.famisafe.child.accessibility.SCAccessibilityService) is Protected by a permission, but the protection level of the permission should be checked.

[MANIFEST](#)

medium Service (com.wondershare.famisafe.kids.notify.MyNotificationMonitorService) is Protected by a permission, but the protection level of the permission should be checked.

[MANIFEST](#)

medium Broadcast Receiver (com.wondershare.famisafe.child.ui.permission.DeviceAdmin) is Protected by a permission, but the protection level of the permission should be checked.

[MANIFEST](#)

[MANIFEST](#)

medium	Broadcast Receiver (com.wondershare.famisafe.kids.receiver.myReceiver) is not Protected.	
medium	Broadcast Receiver (com.wondershare.famisafe.kids.receiver.WakeUpReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.wondershare.famisafe.kids.receiver.WakeUpReceiver\$WakeUpAutoStartReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.wondershare.famisafe.kids.livelocation.helper.AlarmReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.wondershare.famisafe.kids.accessibility.screenview.ScreenAlarmReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.wondershare.famisafe.kids.microrecord.MicroRecordStateAlarmReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.wondershare.famisafe.kids.collect.DataSyncAlarmReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.appsflyer.SingleInstallBroadcastReceiver) 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	Service (com.wondershare.famisafe.kids.MainService) is not Protected.	MANIFEST
medium	Service (com.wondershare.famisafe.kids.service.WatchDogService) is not Protected.	MANIFEST
medium	Service (com.wondershare.famisafe.kids.service.WatchDogService\$WatchDogNotificationService) is not Protected.	MANIFEST
medium	Activity (com.wondershare.famsiafe.billing.PayActivity) is not Protected.	MANIFEST
medium	Activity (com.facebook.CustomTabActivity) 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	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked.	MANIFEST
medium	MD5 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	The App uses an insecure Random Number Generator.	CODE
medium	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	CODE
medium	IP Address disclosure	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

<div>medium</div>	SHA-1 is a weak hash known to have hash collisions.	CODE
<div>medium</div>	This app may contain hardcoded secrets	SECRETS
<div>info</div>	The App logs information. Sensitive information should never be logged.	CODE
<div>info</div>	App can write to App Directory. Sensitive Information should be encrypted.	CODE
<div>secure</div>	This App may have root detection capabilities.	CODE
<div>secure</div>	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	CODE
<div>hotspot</div>	Found 15 critical permission(s)	PERMISSIONS
<div>hotspot</div>	App may communicate to a server (oss-cn-hangzhou.aliyuncs.com) in OFAC sanctioned country (China)	DOMAINS
<div>hotspot</div>	App may communicate to a server (oss.aliyuncs.com) in OFAC sanctioned country (China)	DOMAINS

MobSF Application Security Scorecard generated for

No icon

 (FamiSafe Kids 7.2.7.9592) 