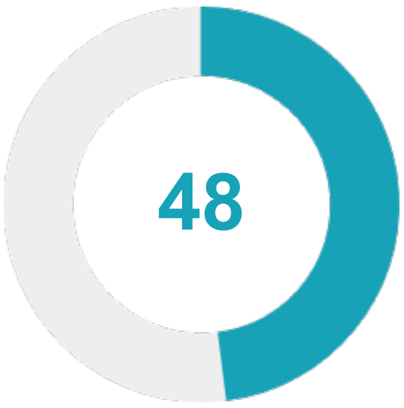
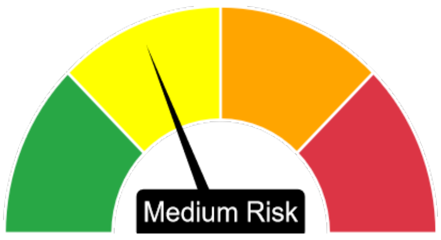
Security Score



Security Score 48/100

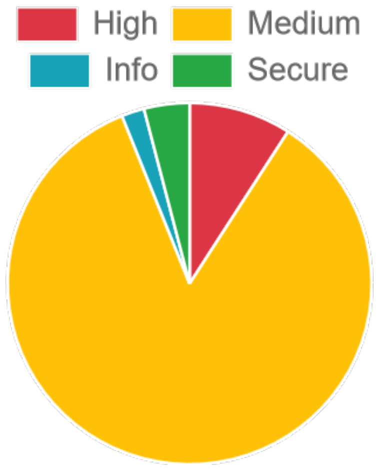
Risk Rating



Grade

A **B** C F

Severity Distribution (%)



Privacy Risk

1

User/Device Trackers

Findings

High	**4**
Medium	**37**
Info	**1**
Secure	**2**
Hotspot	**2**

high App can be installed on a vulnerable upatched Android version — MANIFEST

high Clear text traffic is Enabled For App — MANIFEST

high Calling Cipher.getInstance("AES") will return AES ECB mode by default. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext. — CODE

high Weak Encryption algorithm used — CODE

medium Certificate algorithm might be vulnerable to hash collision — CERTIFICATE

medium Service (com.eset.commoncore.core.FirebaseMessagingService) is not Protected. — MANIFEST

medium Service (com.eset.commoncore.core.accessibility.CoreAccessibilityService) is Protected by a permission, but the protection level of the permission should be checked. — MANIFEST

medium TaskAffinity is set for activity — MANIFEST

medium Activity (com.eset.commongui.gui.ExternalActionsActivity) is not Protected. — MANIFEST

medium Activity (com.eset.parental.gui.PageActivity) is not Protected. — MANIFEST

medium Activity (com.eset.parental.gui.ChildPageActivity) is not Protected. — MANIFEST

medium TaskAffinity is set for activity — MANIFEST

medium TaskAffinity is set for activity — MANIFEST

medium TaskAffinity is set for activity — MANIFEST

medium	TaskAffinity is set for activity	MANIFEST
medium	Activity (com.eset.parental.gui.recovery.ParentalRecoveryActivity) is not Protected.	MANIFEST
medium	Activity (com.eset.next.main.presentation.ExternalConfigActivity) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.eset.parentalcore.core.directboot.DirectBootReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.eset.parentalcore.core.broadcast.ChildCoreReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.eset.commoncore.core.broadcast.CoreReceiver) is not Protected.	MANIFEST
medium	Broadcast Receiver (com.eset.commoncore.core.broadcast.AdminReceiver) is Protected by a permission, but the protection level of the permission should be checked.	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	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.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected.	MANIFEST
medium	High Intent Priority (999)	MANIFEST
medium	High Intent Priority (999)	MANIFEST
medium	High Intent Priority (999)	MANIFEST
medium	SHA-1 is a weak hash known to have hash collisions.	CODE
medium	IP Address disclosure	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	App can read/write to External Storage. Any App can read data written to External Storage.	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 This App may request root (Super User) privileges. CODE

medium MD5 is a weak hash known to have hash collisions. CODE

medium App creates temp file. Sensitive information should never be written into a temp file. 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 This App may have root detection capabilities. CODE

hotspot Found 10 critical permission(s) PERMISSIONS

hotspot Found 1 certificate/key file(s) FILES

MobSF Application Security Scorecard generated for (ESET Parental Control 5.3.6.0)

Version v4.0.6