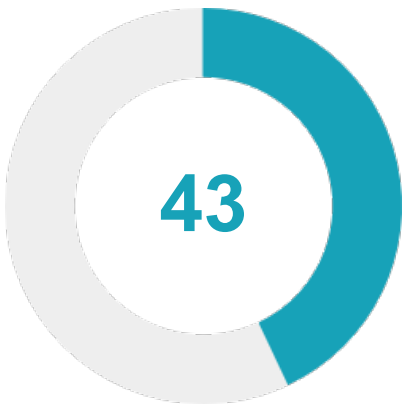
## Security Score

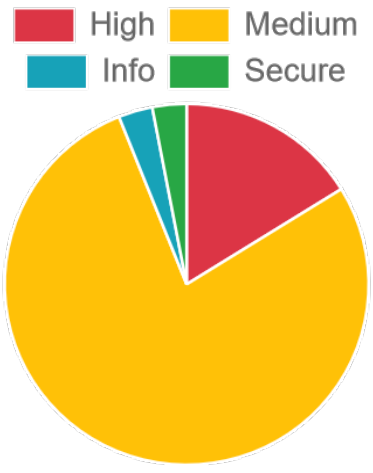



Security Score 43/100

## Risk Rating


Grade


## Severity Distribution (%)




## Privacy Risk


User/Device Trackers

## Findings

| High | Medium | Info | Secure | Hotspot |
|---|---|---|---|---|
| 5 | 24 | 1 | 1 | 1 |

| | |
|---|---|
| high App can be installed on a vulnerable upatched Android version | MANIFEST |
| high Clear text traffic is Enabled For App | MANIFEST |
| high The file or SharedPreference is World Readable. Any App can read from the file | CODE |
| high Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks | CODE |
| high The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks. | CODE |
| medium Application vulnerable to Janus Vulnerability | CERTIFICATE |
| medium Broadcast Receiver (com.mobilefence.family.receiver.SimStateChangedReceiver) is not Protected. | MANIFEST |
| medium Service (com.mobilefence.family.service.TempService) 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 Broadcast Receiver (com.mobilefence.core.knox.KnoxLicenseReceiver) is not Protected. | MANIFEST |
| medium Content Provider (com.mobilefence.family.provider.SharedSettingsProvider) is Protected by a permission, but the protection level of the permission should be checked. | MANIFEST |
| medium Broadcast Receiver (com.mobilefence.family.receiver.AddonCommunicator) is Protected by a permission, but the protection level of the permission should be checked. | MANIFEST |
| medium Broadcast Receiver (com.mobilefence.family.receiver.SACReceiver) is not Protected. | MANIFEST |

| | | |
|---|---|---|
| medium | Broadcast Receiver (com.samsung.android.knox.IntentConverterReceiver) 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 | Activity (com.navercorp.nid.oauth.activity.NidOAuthCustomTabActivity) 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 | High Intent Priority (999) | MANIFEST |
| medium | High Intent Priority (999) | MANIFEST |
| medium | High Intent Priority (999) | MANIFEST |
| medium | Files may contain hardcoded sensitive information like usernames, passwords, keys etc. | 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 | App can read/write to External Storage. Any App can read data written to External Storage. | 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 | MD5 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 |
| hotspot | Found 19 critical permission(s) | PERMISSIONS |

MobSF Application Security Scorecard generated for ( Mobile Fence 5.6.2)