ANDROID STATIC ANALYSIS REPORT

COVID Alert DE (1.2.2)

File Name:	Covid Alert DE_v1.2.2_apkpure.com.xapk
Package Name:	gov.de.covidtracker
Average CVSS Score:	5.9
App Security Score:	30/100 (HIGH RISK)
Scan Date:	Jan. 25, 2022, 1:52 a.m.

FILE INFORMATION

File Name: Covid Alert DE_v1.2.2_apkpure.com.xapk
Size: 4.45MB
MD5: cd6f500478c745b65425bd7e1cce7630
SHA1: 9603202f6b6d8aa3cf084e59e109938bb3b6f42d
SHA256: ea8bedc0ba94f49836d58206f173aba07f137944737f6f003874a1b248a9acbe

APP INFORMATION

App Name: COVID Alert DE
Package Name: gov.de.covidtracker
Main Activity: gov.de.covidtracker.MainActivity
Target SDK: 29
Min SDK: 23
Max SDK:
Android Version Name: 1.2.2
Android Version Code: 24

APP COMPONENTS

Activities: 2
Services: 11
Receivers: 15
Providers: 4
Exported Activities: 0
Exported Services: 3
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-08-07 18:17:20+00:00
Valid To: 2050-08-07 18:17:20+00:00
```

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xeb2c638b0a528b9bfc301d213acb042d3356acc8
Hash Algorithm: sha256
md5: 30bf1c68a693ff775142a3c2b83df140
sha1: 238fddff9b45622f6cb4439085d2e75a10d23086
sha256: 31bd0e7721619800d7ae82b762e6b580a7023595dc1847909488bab51a21d095
sha512: 69910e97d205e4bc734f38170f4fa99245cedf48ad8eba23a8427762e8022a4161fedb2fbb0cc07451df0848a7445f2913ff6ca8c96428c26991d94b40474054
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: b573506da9f88d80c0d26ecb80583021be351addff8c62a06db0fe139116b6b4

STATUS	DESCRIPTION
secure	Application is signed with a code signing certificate
warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
possible Build.SERIAL check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
gov.de.covidtracker.MainActivity	Schemes: gov.de.covidtracker://, https://, Hosts: us-de.en.express,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Broadcast Receiver (com.dieam.reactnativepushnotification.modules.RNPushNotificationBootEventReceiver) is not Protected. An intent-filter exists.	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Broadcast Receiver (ie.gov.tracing.nearby.ExposureNotificationBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.nearby.exposurenotification.EXPOSURE_CALLBACK [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
3	Service (com.google.android.gms.nearby.exposurenotification.WakeUpService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.nearby.exposurenotification.EXPOSURE_CALLBACK [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Service (androidx.work.impl.background.gcm.WorkManagerGcmService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_SERVICE [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
5	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
7	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				f/h/f/k.java h/d/a/b/c/b.java com/franmontiel/persistentcookiejar/persistence/SerializableCookie.java com/bumptech/glide/load/n/q.java h/d/a/b/g/b/m5.java com/swmansion/gesturehandler/react/h.java h/d/a/b/n/a.java f/n/a/b.java f/u/a/b.java f/h/m/b.java net/sqlcipher/database/SQLiteQueryBuilder.java h/d/a/b/g/h/s3.java net/sqlcipher/DefaultDatabaseErrorHandler.java com/bumptech/glide/load/n/b0/e.java h/d/a/b/c/e.java h/d/a/b/g/b/c.java com/swmansion/gesturehandler/react/g.java f/h/n/b.java f/h/e/f/a.java com/dieam/reactnativepushnotification/modules/RNPushNotificationListenerService.java com/bumptech/glide/load/n/c0/b.java h/d/a/b/c/s.java net/sqlcipher/BulkCursorToCursorAdaptor.java com/bumptech/glide/load/o/s.java com/dieam/reactnativepushnotification/modules/RNPushNotificationBootEventReceiver.java f/h/n/t.java h/d/a/b/g/b/f.java f/h/n/a0.java com/bumptech/glide/load/n/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				f/h/e/f/f.java h/d/a/b/g/h/j5.java h/a/a/n/d.java ie/gov/tracing/nearby/ExposureNotificationRepeaterBroadcastReceiver.java h/d/a/b/c/d.java com/bumptech/glide/load/o/f.java f/s/y.java com/bumptech/glide/load/n/i.java i/a/a/c.java com/bumptech/glide/load/m/j.java f/j/b/c.java com/bumptech/glide/load/o/d.java h/d/a/b/f/d.java net/sqlcipher/database/SQLiteProgram.java f/h/n/s.java net/sqlcipher/database/SqliteWrapper.java h/d/a/b/g/b/l.java com/bumptech/glide/load/n/c0/a.java h/d/a/b/b/a.java h/d/a/b/g/e/o.java com/bumptech/glide/manager/k.java i/a/i/a.java f/h/f/e.java com/dieam/reactnativepushnotification/modules/RNPushNotificationActions.java f/a/o/g.java net/sqlcipher/database/SQLiteContentHelper.java h/d/a/b/g/b/k.java h/d/a/c/y/b.java h/d/a/b/c/v.java h/d/a/b/g/l/a.java h/d/a/b/c/u.java com/bumptech/glide/manager/e.java com/dieam/reactnativepushnotification/modules/b.java f/h/f/c.java com/bumptech/glide/load/o/t.java f/h/n/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 (high) CWE: CWE-532 Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/bumptech/glide/load/n/b0/i.java com/dieam/reactnativepushnotification/modules/RNPushNotificationPublisher.java h/d/a/b/l/a.java com/bumptech/glide/load/p/g/a.java h/d/a/b/g/g/l.java h/d/a/b/c/i.java com/bumptech/glide/load/m/l.java h/d/a/b/g/b/m.java f/h/f/f.java f/t/a/a/i.java ie/gov/tracing/nearby/ExposureNotificationBroadcastReceiver.java h/a/a/r/l/a.java net/sqlcipher/database/SQLiteOpenHelper.java f/a/k/a/a.java h/d/a/b/g/h/t3.java net/sqlcipher/database/SQLiteCompiledSql.java h/d/a/b/c/j.java com/bumptech/glide/load/o/c.java com/bumptech/glide/load/p/g/d.java f/h/n/h.java f/h/n/b0/c.java f/h/n/v.java com/dieam/reactnativepushnotification/modules/RNPushNotification.java com/dieam/reactnativepushnotification/modules/e.java f/r/a/c.java h/a/a/m/e.java com/dieam/reactnativepushnotification/modules/a.java h/d/a/b/k/b/a.java com/bumptech/glide/load/n/k.java com/dieam/reactnativepushnotification/modules/c.java h/c/i/c/f.java expo/modules/filesystem/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				net/sqlcipher/database/SQLiteDebug.java com/bumptech/glide/load/p/c/s.java net/sqlcipher/database/SQLiteDatabase.java h/d/a/b/g/b/w5.java com/bumptech/glide/load/p/c/c.java com/dieam/reactnativepushnotification/modules/f.java org/unimodules/adapters/react/views/a.java com/bumptech/glide/load/n/a0/j.java com/th3rdwave/safeareacontext/g.java h/a/a/m/d.java l/a/a/c.java com/bumptech/glide/manager/SupportRequestManagerFragment.java f/s/i0.java f/h/k/d.java com/bumptech/glide/load/p/c/f.java h/d/a/c/n/a.java f/h/f/g.java com/bumptech/glide/load/m/b.java f/h/e/a.java f/h/f/j.java com/bumptech/glide/load/m/o/c.java f/q/a/c.java h/d/a/b/g/h/e5.java h/d/a/a/i/v/a.java h/a/a/c.java com/bumptech/glide/load/p/g/j.java net/sqlcipher/database/SQLiteQuery.java h/d/a/b/g/l/d.java h/d/a/b/g/h/p.java ie/gov/tracing/common/g.java com/bumptech/glide/manager/f.java com/bumptech/glide/load/p/c/l.java net/sqlcipher/DatabaseUtils.java h/d/a/c/x/d.java net/sqlcipher/AbstractCursor.java com/bumptech/glide/load/p/c/h.java h/a/a/p/h.java com/bumptech/glide/load/n/z.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				f/h/k/i.java com/bumptech/glide/load/n/a0/k.java h/d/a/c/l/h.java com/bumptech/glide/load/p/c/i.java com/bumptech/glide/manager/n.java gov/de/covidtracker/MainActivity.java com/bumptech/glide/manager/l.java h/d/a/b/g/b/a6.java f/h/e/f/b.java
2	This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	info	CVSS V2: 0 (info) OWASP MASVS: MSTG-CRYPTO-1	net/sqlcipher/database/SupportHelper.java
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CVSS V2: 7.4 (high) CWE: CWE-312 Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/bumptech/glide/load/h.java com/pedrouid/crypto/RandomBytesModule.java com/toyberman/RNSslPinningModule.java com/bumptech/glide/load/n/x.java com/bumptech/glide/load/n/d.java com/bumptech/glide/load/n/p.java org/unimodules/adapters/react/NativeModulesProxy.java
4	App can read/write to External Storage. Any App can read data written to External Storage.	high	CVSS V2: 5.5 (medium) CWE: CWE-276 Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	h/c/d/i/a.java h/c/b/b/a.java f/h/e/b.java f/h/e/a.java
5	App creates temp file. Sensitive information should never be written into a temp file.	warning	CVSS V2: 5.5 (medium) CWE: CWE-276 Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	h/c/b/b/a.java h/d/a/b/j/b.java com/toyberman/b/a.java
6	The App uses an insecure Random Number Generator.	warning	CVSS V2: 7.5 (high) CWE: CWE-330 Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	n/b/d/a/d.java k/b0/a.java k/b0/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	App can write to App Directory. Sensitive Information should be encrypted.	info	CVSS V2: 3.9 (low) CWE: CWE-276 Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	i/a/h/c.java
8	IP Address disclosure	warning	CVSS V2: 4.3 (medium) CWE: CWE-200 Information Exposure OWASP MASVS: MSTG-CODE-2	n/b/a/z1/a.java n/b/a/c2/e/b.java n/b/a/e2/g.java n/b/a/d2/j.java n/b/a/d2/x.java n/b/a/a2/e.java
9	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.	warning	CVSS V2: 5.9 (medium) CWE: CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	f/q/a/g/a.java net/sqlcipher/database/SQLiteDatabase.java h/d/a/a/i/x/j/h0.java com/reactnativecommunity/asyncstorage/e.java h/d/a/a/i/x/j/b0.java
10	SHA-1 is a weak hash known to have hash collisions.	warning	CVSS V2: 5.9 (medium) CWE: CWE-327 Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	h/c/d/k/c.java
11	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	CVSS V2: 0 (info) OWASP MASVS: MSTG-NETWORK-4	ie/gov/tracing/network/d.java com/toyberman/b/a.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['bluetooth', 'network connectivity'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.
12	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption not in accordance with FCS_COP.1.1(1), AES-ECB mode is being used.
13	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
14	FCS_COP.1.1(3)	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
15	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
16	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
17	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
18	FCS_CKM.1.1(2)	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
expo.io	good	**IP:** 34.132.55.135 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
schemas.android.com	good	No Geolocation information available.
github.com	good	**IP:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.zetetic.net	good	**IP:** 13.224.7.17 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

URLS

URL	FILE
https://expo.io	i/a/j/i.java
http://schemas.android.com/apk/res/android	f/h/e/f/g.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	j/a/b.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	j/a/g/e.java
data:image	com/bumptech/glide/load/o/e.java
https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenStackFragment.java
https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenFragment.java
https://www.zetetic.net/sqlcipher/ https://www.zetetic.net/sqlcipher/license/ https://github.com/sqlcipher/android-database-sqlcipher	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"library_android_database_sqlcipher_author" : "Zetetic, LLC"
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.4.5 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.