ANDROID STATIC ANALYSIS REPORT

SecuMobileIsen (1.0)

File Name:	app-release.apk
Package Name:	com.isen.secumobileisen
Average CVSS Score:	7.5
App Security Score:	100/100 (LOW RISK)
Trackers Detection:	1/285

FILE INFORMATION

File Name: app-release.apk
Size: 4.07MB
MD5: 6b18c39ea588cead89e4efffbf51d344
SHA1: 7eb1d2f3266c8ab45fe8d8b70d587e9cf887a439
SHA256: 9eb4602b24337f38d0bc7424ccc5f005aeba985073158ce0ca94aeb49d2b8a19

APP INFORMATION

App Name: SecuMobileIsen
Package Name: com.isen.secumobileisen
Main Activity: com.isen.secumobileisen.LoginActivity
Target SDK: 29
Min SDK: 26
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 10
Services: 6
Receivers: 4
Providers: 2
Exported Activities: 1
Exported Services: 0
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: False
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=OI, ST=Oui, L=Oui, O=Oui, OU=Oui, CN=Oui
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-03-04 14:23:21+00:00
Valid To: 2045-02-26 14:23:21+00:00
Issuer: C=OI, ST=Oui, L=Oui, O=Oui, OU=Oui, CN=Oui
Serial Number: 0x3f067a
Hash Algorithm: sha256
md5: 70df4297f63882a15de9eab4623827c2
sha1: 1227d5aefca25031513dd1f3d9a78a32db9d2894
sha256: b1e73ce50ba0bd6e7621ef2023a116ca7d6ba1017ea587d55ba84a1ecfde0610
sha512:

4ce85748f109c28f0d1ab1f9c8a1509d891a051adf5bef3d630a1d2f507d9d744e66c9881b4cf52cbf0e6288762acf6922b2acdfc3312497f9b31301888c8da8

PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 773624f6f9ba9ff93c46c1de45cd08d04878f31abbd0a7d3a912c8985b7aeec9

Certificate Status: Good
Description: Certificate looks good.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	dangerous	Unknown permission from android reference	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check Build.TAGS check FINDINGS: Compiler — DETAILS: dx

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Activity (com.google.firebase.auth.internal.FederatedSignInActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.firebase.auth.api.gms.permission.LAUNCH_FEDERATED_SIGN_IN [android:exported=true]	high	An Activity 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.
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.
Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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

ISSUE	SEVERITY	CVSS	CWE	OWASP	FILES

ISSUE	SEVERITY	CVSS	CWE	OWASP	FILES
The App logs information. Sensitive information should never be logged.	info	7.5 high	CWE-532		com/firebase/ui/firestore/FirestoreRecyclerAdapter.java com/firebase/ui/firestore/paging/FirestoreDataSource.java com/firebase/ui/firestore/paging/FirestorePagingAdapter.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
securitemobileisen.firebaseio.com	good	**IP:** 35.201.97.85 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

URLS

URL	FILE
https://securitemobileisen.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://securitemobileisen.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

TRACKER	URL
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49

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 v3.0.4 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.