ANDROID STATIC ANALYSIS REPORT

SecuGerbisNucleaires (1.0)

File Name:	app-release.apk
Package Name:	fr.isen.gerbisnucleaires.secugerbisnucleaires
Average CVSS Score:	4.9
App Security Score:	80/100 (LOW RISK)

FILE INFORMATION

File Name: app-release.apk
Size: 2.19MB
MD5: 0cd65663cc89de05c9f95bf5597320c9
SHA1: 39a594330eb74bd7d798d016b50cc13cb7a423b3
SHA256: 2cf40ba4d8e73249121e4eee22d5f63094070b185d21b7c61bf2ab11b23ffc5f

APP INFORMATION

App Name: SecuGerbisNucleaires
Package Name: fr.isen.gerbisnucleaires.secugerbisnucleaires
Main Activity: fr.isen.gerbisnucleaires.secugerbisnucleaires.LoginActivity
Target SDK: 29
Min SDK: 28
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 14
Services: 1
Receivers: 0
Providers: 2
Exported Activities: 2
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: False
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=33, ST=PACA, L=Toulon, O=ISEN, OU=Cyber, CN=Gerbis Nucléaires
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-03-06 07:51:47+00:00
Valid To: 2045-02-28 07:51:47+00:00
Issuer: C=33, ST=PACA, L=Toulon, O=ISEN, OU=Cyber, CN=Gerbis Nucléaires
Serial Number: 0x69e82af6
Hash Algorithm: sha256
md5: 2c49e5a20b1178d5c7929a6d103255ce
sha1: 80a3032b7546f292c2202d5723249e33557898f8
sha256: 9beab3cbb2bf80b88b876a118a9d3bf1492d6438a475694296bd202bdf9fac2c
sha512:
feafa6727e5d3682e50bef1b30948f1d6be01ff8e1f95f09ad7d9942e393e9479a622ca03b385d1ff1d825dacf6b76419a01a422ccd10b2a86b02e4b1c474972

PublicKey Algorithm: rsa

Bit Size: 2048
Fingerprint: 6c6d2de2910ab7e6b10f8a5c0f7a23f24f7889ff1d32cc5f1ada6ccd1a41dd34

Certificate Status: Good
Description: Certificate looks good.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_BIOMETRIC	normal		Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead
android.permission.INTERNET	dangerous	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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check Build.TAGS check possible ro.secure check FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Activity (androidx.biometric.DeviceCredentialHandlerActivity) is not Protected. [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.

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.

</> CODE ANALYSIS

ISSUE	SEVERITY	CVSS	CWE	OWASP	FILES
The App logs information. Sensitive information should never be logged.	info	7.5 high	CWE-532		b/a/d/j.java b/f/b/b/a.java b/f/c/b.java b/f/c/d.java b/f/c/e.java b/f/f/b.java b/f/i/a.java b/f/j/d.java b/f/j/i.java b/f/j/u.java b/f/j/C/b.java b/g/b/l.java b/j/a/d.java b/l/e0.java c/b/a/a/a/i.java c/b/a/a/a/h.java c/b/a/a/a/p.java c/b/a/a/a/d.java c/b/a/a/a/q.java c/b/a/a/a/e.java c/b/a/a/a/k/a.java c/b/a/a/c/c/m0.java c/b/a/a/d/b/a.java c/b/a/b/c/g.java c/b/a/b/j/f.java c/b/b/h.java c/c/a/d/a.java fr/isen/gerbisnucleaires/secugerbisnucleaires/LoginActivity.java fr/isen/gerbisnucleaires/secugerbisnucleaires/b.java

ISSUE	SEVERITY	CVSS	CWE	OWASP	FILES
This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	2.3 low	CWE-327		b/b/a/b/d.java b/b/a/b/h.java b/c/j.java b/c/i.java b/c/k.java b/c/d.java b/c/n.java b/f/j/B.java b/f/j/C/b.java b/f/j/C/e.java b/l/O.java b/l/i0.java c/b/a/a/c/c/C0208j.java c/b/a/a/c/c/C0213o.java c/b/a/a/c/c/C0221x.java c/b/a/b/c/g.java c/b/a/b/c/h.java c/b/b/h.java c/b/b/r/a.java fr/isen/gerbisnucleaires/secugerbisnucleaires/AddPatientActivity.java fr/isen/gerbisnucleaires/secugerbisnucleaires/B/b.java fr/isen/gerbisnucleaires/secugerbisnucleaires/B/a.java fr/isen/gerbisnucleaires/secugerbisnucleaires/C/h.java fr/isen/gerbisnucleaires/secugerbisnucleaires/C/l/a.java fr/isen/gerbisnucleaires/secugerbisnucleaires/C/l/b.java
This App may request root (Super User) privileges.	high	0 info	CWE-250		c/c/a/a.java
This App may have root detection capabilities.	secure	0 info			c/c/a/b.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
secus-gerbis-nucleaires.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
http://localhost	c/b/a/a/c/c/w0.java

URL	FILE
https://secus-gerbis-nucleaires.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://secus-gerbis-nucleaires.firebaseio.com/.json	insecure Firebase DB is exposed publically.

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	c/b/a/a/a/v.java
allan.duee@isen.yncrea	fr/isen/gerbisnucleaires/secugerbisnucleaires/SignUpActivity.java

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.