MOBSF

ANDROID STATIC ANALYSIS REPORT

PinLock Middle (1.0)

File Name:	935550de0691ca4762d74b3cdd372f18 (1).apk
Package Name:	com.andrognito.pinlockviewappMiddle
Scan Date:	April 8, 2024, 2:59 p.m.
App Security Score:	36/100 (HIGH RISK)
Grade:	C

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	2	1	1	0

FILE INFORMATION

File Name: 935550de0691ca4762d74b3cdd372f18 (1).apk
Size: 1.53MB
MD5: 935550de0691ca4762d74b3cdd372f18
SHA1: 6ce502e9e4b97b488a638dbf184984ad3c08d099
SHA256: dae0cb40e7d936c05d031a2dcf692ccc57e0c407395b5276bbb308771b6064a8

APP INFORMATION

App Name: PinLock Middle
Package Name: com.andrognito.pinlockviewappMiddle
Main Activity: com.andrognito.pinlockapp.SampleActivity
Target SDK: 25
Min SDK: 11
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

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

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-04-03 14:42:00+00:00
Valid To: 2050-08-19 14:42:00+00:00
Issuer: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Serial Number: 0x6b4392da0b5a5f1d
Hash Algorithm: sha384
md5: 52fe929b26a461308a570434e18c1990
sha1: c39e3c77fc75d538794e270a0b50f8da9b66d439
sha256: 5a8b5ee4e3a31c3d36d23dbde2507ee1835a5a854df8cc3cadd309beaba65aa7
sha512: 6920b76839bb4205d83f00830ceee13777f5fbdf0c01f4394aaa066988fa0572181de7542e2664f6665a785cac1adca7df99d76694086668e58aba68765e544a
Found 1 unique certificates

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dexlib 2.x</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: 2 | WARNING: 1 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 3.0, [minSdk=11]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

</> CODE ANALYSIS

HIGH: **1** | WARNING: **1** | INFO: **1** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/andrognito/pinlockapp/SampleActivity.java com/andrognito/pinlockview/ShuffleArrayUtils.java
2	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/andrognito/pinlockapp/BuildConfig.java com/andrognito/pinlockview/BuildConfig.java com/andrognito/pinlockviewapp/BuildConfig.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/androgniito/pinlockapp/SampleActivity.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	0/24	
Other Common Permissions	0/45	

Malware Permissions:
Top permissions that are widely abused by known malware.

Other Common Permissions:
Permissions that are commonly abused by known malware.

Report Generated by - MobSF v3.9.8 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.