MOBSF

ANDROID STATIC ANALYSIS REPORT

Antimine (8.3.8)

File Name:	installer186.apk
Package Name:	dev.lucanlm.antimine
Scan Date:	May 31, 2022, 2:37 p.m.
App Security Score:	64/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	4	1	1	1

FILE INFORMATION

File Name: installer186.apk
Size: 4.94MB
MD5: a8290bd241c75183658208794ea9d97a
SHA1: 7548eb7396c856cba9b6d5033e6959b642c46b38
SHA256: 11b5ce4f221d468521177fc5275feb8f425eb17346ded32827b2d5b15a342067

APP INFORMATION

App Name: Antimine
Package Name: dev.lucanlm.antimine
Main Activity: dev.lucasnlm.antimine.splash.SplashActivity
Target SDK: 30
Min SDK: 21
Max SDK:
Android Version Name: 8.3.8
Android Version Code: 803081

APP COMPONENTS

Activities: 8
Services: 1
Receivers: 0
Providers: 2
Exported Activities: 1
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-05-22 20:05:29+00:00
Valid To: 2047-10-08 20:05:29+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x63f450d8
Hash Algorithm: sha256
md5: dab809a5cf0678ff48dc67b36da838fe
sha1: c4052ecbc22315749e2561d065451d8401ed8d34
sha256: 5b7e1417bf2bbea68064a0a18df604d4712fd6be048ce66a6f7897376fc1699e
sha512: aebf257ecbd649b95064d225b2deeb25cf53830d0ad2b39c1520d04c481365f7bf12f59d003663249679f260cdd84eb93604f71f6465c688f4770788f67c1605
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 03a001bb4da207df05a9230ece53c05211f2c7b75e811e3b034f17d7aaec9522

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: r8

FILE	DETAILS
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
dev.lucasnlm.antimine.splash.SplashActivity	Schemes: http://, https://, Hosts: www.lucasnlm.dev, Paths: /, /antimine,
dev.lucasnlm.antimine.GameActivity	Schemes: antimine://, Hosts: new-game, load-game, retry-game,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Activity (dev.lucasnlm.antimine.GameActivity) is not Protected. An intent-filter exists.	warning	An Activity 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 Activity is explicitly exported.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	dev/lucasnlm/antimine/tutorial/view/TutorialAreaAdapter.java org/koin/android/logger/AndroidLogger.java dev/lucasnlm/antimine/common/level/widget/FixedGridLayoutManager.java dev/lucasnlm/antimine/splash/SplashActivity$onCreate$1.java dev/lucasnlm/antimine/splash/viewmodel/SplashViewModel.java org/koin/core/time/MeasureKt.java dev/lucasnlm/antimine/common/level/view/AreaAdapter.java dev/lucasnlm/antimine/GameActivity.java dev/lucasnlm/antimine/core/analytics/DebugAnalyticsManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	dev/lucasnlm/antimine/share/ShareManager.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 use no 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 generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to no hardware resources.
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 no network communications.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.paypal.com	ok	**IP:** 151.101.129.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
crowdin.com	ok	**IP:** 44.199.129.167 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

---

Report Generated by - MobSF v3.5.2 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.