MOBSF

ANDROID STATIC ANALYSIS REPORT

Planes Android (0.3.10.1)

File Name:	installer219.apk
Package Name:	com.planes.android
Scan Date:	May 31, 2022, 2:57 p.m.
App Security Score:	60/100 (LOW RISK)
Grade:	

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	6	1	1	0

FILE INFORMATION

File Name: installer219.apk
Size: 2.4MB
MD5: db83f51af2947727314bd0e23c15d536
SHA1: d181dadc1e3ebb46de7604d6b1365595a61f14ce
SHA256: f1c90b58ed6bf39affd9a1246b87fa4a5b0890dff18400ab211c84d044a11bec

APP INFORMATION

App Name: Planes Android
Package Name: com.planes.android
Main Activity: com.planes.android.PlanesAndroidActivity
Target SDK: 29
Min SDK: 16
Max SDK:
Android Version Name: 0.3.10.1
Android Version Code: 14

APP COMPONENTS

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

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=Cristian Cucu
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-02-27 10:08:21+00:00
Valid To: 2044-02-21 10:08:21+00:00
Issuer: CN=Cristian Cucu
Serial Number: 0x3bb0b9c5
Hash Algorithm: sha256
md5: bc6382194504b659fb68a8e3271f0d3b
sha1: 5edfccf78b133aefa03d66c7268afbed015f570e
sha256: 207ab253ca2d2848d91a7606ec81c5ae0f9dd488320d24fe2bbacc05fea13b29
sha512: 721a0166ae5684e70e02670bcdfe892ab9b5fad4d7d8f95ba270eab8d6e1afeb94c929041f7e8c7b0ac659abafe8defd6761d1ad4911aca9102d638a6bf6eae7
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 7fd75892da01e3c5a6f8043e1216c984c285e02ebcffcebcc555cd2ba0b0abb1

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Compiler — DETAILS: r8

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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

NO	ISSUE	SEVERITY	STANDARDS	FILES

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	com/planes/javafx/PlaneRoundJavaFx.java junit/runner/Version.java com/planes/android/OptionsActivity.java junit/textui/TestRunner.java junit/runner/BaseTestRunner.java com/planes/android/GameBoard.java com/planes/android/PreferencesService.java com/planes/android/PlanesAndroidActivity.java
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/planes/android/BuildConfig.java
3	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	org/junit/rules/TemporaryFolder.java
4	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/planes/common/Plane.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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 ['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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.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.youtube.com	ok	**IP:** 142.250.179.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
axa951.wixsite.com	ok	**IP:** 35.246.6.109 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"draws" : "Draws"

POSSIBLE SECRETS
"draws" : "Egalitate"

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.