

## ANDROID STATIC ANALYSIS REPORT



Planes Android (0.3.10.1)

File Name:	installer146.apk
Package Name:	com.planes.android
Scan Date:	May 31, 2022, 3:38 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	

### FINDINGS SEVERITY

<b>派</b> HIGH	▲ MEDIUM	<b>i</b> INFO	✓ SECURE	≪ HOTSPOT
1	5	1	1	0

#### FILE INFORMATION

File Name: installer146.apk

Size: 2.41MB

MD5: 93f175144704dc48725208e7d51a0018

**SHA1**: ba4ae85b6de6f1110b94b587f7e9f7b8817e0e34

SHA256: c05aa829aa74763354090cf6cce732d8d5881f7902f1a6f842b94638b8bfda82

### **i** 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

#### **EE** APP COMPONENTS

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

Exported Activities: O Exported Services: O Exported Receivers: O Exported Providers: O

## **\*** CERTIFICATE INFORMATION

APK is signed v1 signature: True v2 signature: False v3 signature: False

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 19:59:43+00:00 Valid To: 2047-10-08 19:59:43+00:00

Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Serial Number: 0x52fb7dbe Hash Algorithm: sha256

md5: 09927d2b3aa9373a30fbf6e763ec20a7

sha1: 0eb85eb48b08dbb821ce715d7952d14f8c2ed455

sha256: 69b2beea fe 61c23 ef 6 ca 9 df d704f 355 ed ced 2560379 ee 271a1f 2c3 ed b4b3918c

sha512: 428b7f1af40186070b357adc54d83aab1c39e3a3de4ff2dedebd75ba7f0e3e45f74bb17f292dab6ff96bb2e2051e933605791ca613836a195e798a3e29758b2a

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

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	high	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.

## **命 APKID ANALYSIS**

FILE	DETAILS		
classes.dex	FINDINGS	DETAILS	
Classes.dex	Compiler	r8	



NO SCOPE SEVERITY DESCRIPTION
-------------------------------

## **Q** MANIFEST ANALYSIS

Ν	10	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/android/OptionsActivity.jav a junit/textui/TestRunner.java junit/runner/BaseTestRunner.java com/planes/android/GameBoard.java com/planes/android/PreferencesService. java junit/runner/Version.java com/planes/javafx/PlaneRoundJavaFx.ja va com/planes/android/PlanesAndroidActiv ity.java
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	org/junit/rules/TemporaryFolder.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/planes/android/BuildConfig.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.

# **Q 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.

© 2022 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.