ANDROID STATIC ANALYSIS REPORT

Flight Mode (1.1)

File Name:	installer198.apk
Package Name:	org.aja.flightmode
Scan Date:	May 30, 2022, 4:24 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	2	0	1	1

FILE INFORMATION

File Name: installer198.apk
Size: 0.06MB
MD5: f0b5944cc4802e04539150e6570333c3
SHA1: 0b3970f313bb3a64ed9854c2d1f20c6f6dbf3cab
SHA256: 4c74c84fc7528237de1dc94b3295374d72c1f43f0a115c0798b9063a249053ba

APP INFORMATION

App Name: Flight Mode
Package Name: org.aja.flightmode
Main Activity:
Target SDK: 16
Min SDK: 4
Max SDK: 16
Android Version Name: 1.1
Android Version Code: 2

APP COMPONENTS

Activities: 0

Services: 0

Receivers: 1

Providers: 0

Exported Activities: 0

Exported Services: 0

Exported Receivers: 1

Exported Providers: 0

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: 2013-06-26 13:53:24+00:00

Valid To: 2040-11-11 13:53:24+00:00

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

Serial Number: 0x23e61fbb

Hash Algorithm: sha256

md5: 7d2b79ce02b1264ec71096c15561cee8

sha1: 3733b0ccd450f6c9b0b4066a8311c1e37fe53002

sha256: 384748c8a1d04f57e35a57901f54376471fcd6970e447790ea98c3cc24b1c255

sha512: ac1a076e3a7d2481896b7b991819816b74fe5b89646a03b89c5490179e433752fb8306fe3d7f9313514470396ba5415bca60c3e09b976b4955f8aab013233781

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.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx</td></tr></table></td></tr>
</table>

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	Broadcast Receiver (FlightmodeAppWidgetProvider) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver 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 Broadcast Receiver is explicitly exported.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
2	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to no hardware resources.
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has no network communications.
6	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files in non-volatile memory.
7	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does not encrypt any data in traffic or does not transmit any data between itself and another trusted IT product.

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.