

ANDROID STATIC ANALYSIS REPORT



IWS (07.00.00)

File Name:	installer148.apk
Package Name:	net.basov.lws.fdroid
Scan Date:	May 31, 2022, 7:58 a.m.
App Security Score:	45/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
2	3	1	1	1

FILE INFORMATION

File Name: installer148.apk

Size: 0.05MB

MD5: 1faec76a2993d9e2d9e84146d5c690c3

SHA1: 11f487f31b40f3a7317e58b0c5596c3f3d7d8e18

SHA256: d2b786806f3b294cedfff483d625ee163e3edee047fc454923685a9936ec2b50

i APP INFORMATION

App Name: IWS

Package Name: net.basov.lws.fdroid
Main Activity: net.basov.lws.StartActivity

Target SDK: 28 Min SDK: 10 Max SDK:

Android Version Name: 07.00.00 Android Version Code: 70000

EE APP COMPONENTS

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

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



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: 2018-10-22 12:36:45+00:00 Valid To: 2046-03-09 12:36:45+00:00

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

Serial Number: 0x129fa579 Hash Algorithm: sha256

md5: d92c096492833f58524982422ea81147

sha1: b9c2c30ce96c06cfc9b2f82a1af16f98bbb6e3ad

sha256: 8f18291696606bf90563a9ccf9f1e34868d7a979e554b3f3442826d4b9ad8035

sha512: 37b7d05bdae3cb255e029035711bd458c27c1834f072d3978ca623c466ccca609f4396227bd6af3db1c720fedb52c4fc4c9b189df86e863911e34b374c2b52d3

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_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

M APKID ANALYSIS

FILE	DETAILS
------	---------

FILE	DETAILS		
	FINDINGS	DETAILS	
classes.dex	Compiler	dx	

△ NETWORK SECURITY

NO SCOPE SEVERITY DESCRIPTION

Q 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	Launch Mode of Activity (net.basov.lws.StartActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

</> 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	net/basov/lws/b.java net/basov/lws/ServerService.java net/basov/lws/a.java net/basov/lws/StartActivity.java net/basov/lws/PreferencesActivity.j ava
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	net/basov/lws/ServerService.java net/basov/lws/StartActivity.java
3	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	net/basov/lws/StartActivity.java

■ 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.
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 ['network connectivity'].
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated 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	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.
8	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.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
github.com	ok	IP: 140.82.121.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	IP: 128.30.52.100 Country: United States of America Region: Massachusetts City: Cambridge Latitude: 42.365078 Longitude: -71.104523 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.

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