MOBSF

ANDROID STATIC ANALYSIS REPORT

MOROway (6.3.3)

File Name:	installer49.apk
Package Name:	de.moroway.oc
Scan Date:	May 31, 2022, 10:46 a.m.
App Security Score:	42/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	1	1	1	0

FILE INFORMATION

File Name: installer49.apk
Size: 4.75MB
MD5: d9a287936f52ce3608f43990f17cb4dc
SHA1: 4139d9245800a541a54dba81ee910033976e68db
SHA256: 14b8f2c1161f5500ad255438534a4e7b85c37173888af8747ff25ddea14f5c3f

APP INFORMATION

App Name: MOROway
Package Name: de.moroway.oc
Main Activity: de.moroway.oc.MainActivity
Target SDK: 29
Min SDK: 22
Max SDK:
Android Version Name: 6.3.3
Android Version Code: 60303

APP COMPONENTS

Activities: 1
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: 2020-08-21 14:23:33+00:00
Valid To: 2048-01-07 14:23:33+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x7381eedb
Hash Algorithm: sha256
md5: 99552075223b6071ba455a56da32fa42
sha1: a4d84a5a69babed15ce42516638976a08983cbc6
sha256: 0708287553d68ff8eed665b8430743e55b15a9d29ee50b5ea0e8ab359c52845b
sha512: 83d99b8bc03eec24dc9a7723c2c5d516e175567f5c901904beda4d5c30affe01ee2461c9ca82818d97e48463025796e1107e73cecd7081e46ac833f626ce0eeb

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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: DETAILS Anti Debug Code: Debug.isDebuggerConnected() check Compiler: r8

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
de.moroway.oc.MainActivity	Schemes: https://, http://, Hosts: app.moroway.de,

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.
2	Broadcast Receiver (com.borismus.webintent.WebIntent$ReferralReceiver) is not Protected. [android:exported=true]	high	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.

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	cordova/plugins/screenorientation/CDVOrientation.java com/borismus/webintent/WebIntent.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 invoke platform-provided 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 ['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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files in non-volatile memory.
8	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.
9	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
10	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.

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.