

ANDROID STATIC ANALYSIS REPORT



\Pi Lona (1.0.0)

File Name:	installer3850.apk
Package Name:	io.github.lufte.lona
Scan Date:	May 31, 2022, 7:06 p.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
1	1	0	1	0

FILE INFORMATION

File Name: installer3850.apk

Size: 1.77MB

MD5: 0a394fec71e61abd953320b0649a1b55

SHA1: 96e4a8646ada995bff93d731857f4a133333f8ee

SHA256: 9a51fe6b46ea07fd0ed2bd9872763f5373cb2da861bbafae47d644d46dd91a31

i APP INFORMATION

App Name: Lona

Package Name: io.github.lufte.lona

Main Activity: io.github.lufte.lona.MainActivity

Target SDK: 27 Min SDK: 19 Max SDK:

Android Version Name: 1.0.0 Android Version Code: 10000

EE APP COMPONENTS

Activities: 1 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: 2019-01-15 12:15:38+00:00 Valid To: 2046-06-02 12:15:38+00:00

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

Serial Number: 0x46c8da Hash Algorithm: sha256

md5: 1cf6a8625e48009b2e9f95f88ad7e7a2

sha1: d1a975913c55d92cc0c38911a6fa898b579f32fe

sha256: 2445d1321c1409bfb57428f06ebc1049bfe156f76b1b5815c0fc216df00da0cb

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.

命 APKID ANALYSIS

FILE	DETAILS		
	FINDINGS	DETAILS	
classes.dex	Anti Debug Code	Debug.isDebuggerConnected() check	
	Compiler	dx (possible dexmerge)	
	Manipulator Found	dexmerge	

△ NETWORK SECURITY

NO SCOPE SEVERITY DESCRIPTION

Q 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	
--	----------	----------	-----------	-------	--

■ 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.

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 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.

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