

ANDROID STATIC ANALYSIS REPORT



• NitroShare (0.4.0.38)

File Name:	installer390.apk
Package Name:	net.nitroshare.android
Scan Date:	May 31, 2022, 2:32 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
1	5	1	1	1

FILE INFORMATION

File Name: installer390.apk

Size: 2.49MB

MD5: 4554779695991e9f58701fa436296829

SHA1: 8bc710feacb51ba4bb92dab0adcbef9dbd36b750

SHA256: fb2fe714814d1a0cc918e606b6d51f650828df315ea051472b8c98fa614ada9f

i APP INFORMATION

App Name: NitroShare

Package Name: net.nitroshare.android

 $\textbf{\textit{Main Activity}}: net. nitroshare. and roid. ui. transfer. Transfer Activity$

Target SDK: 27 Min SDK: 16 Max SDK:

Android Version Name: 0.4.0.38 Android Version Code: 39

EE APP COMPONENTS

Activities: 6 Services: 1 Receivers: 1 Providers: 0

Exported Activities: 1 Exported Services: 0 Exported Receivers: 1 Exported Providers: 0



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: 2018-02-28 11:05:01+00:00 Valid To: 2045-07-16 11:05:01+00:00

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

Serial Number: 0x2be4c66b Hash Algorithm: sha256

md5: d8537ae9d9f966446b0fefd45cb9e50a

sha1: e819df563c1b4ebefd0d7c37b54b8eebf65ee8ac

sha256; 965cc77c06acc120333fe3489b5ed1160b6d57911245316b2eb09b2a0723ed84

sha512: 213ea64483510fa191082d89703698c39323065772e906a1ee2ceb2bd209877c5ae9f41f2e2f7646db5c794104786f7a5526046b43ad4a79a77f3850d420751c

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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.

ক্ল APKID ANALYSIS

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

FILE	DETAILS		
classes.dex	FINDINGS	DETAILS	
classes.ucx	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	Activity (net.nitroshare.android.ui.ShareActivity) is not Protected. An intent-filter exists.	warning	An Activity 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 Activity is explicitly exported.
3	Broadcast Receiver (net.nitroshare.android.util.StartReceiver) 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
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/github/paolorotolo/appintro/AppIntroB ase.java net/nitroshare/android/ui/ShareActivity.java com/b/a/ae.java android/a/b/i.java net/nitroshare/android/ui/transfer/Transfer Activity.java net/nitroshare/android/ui/transfer/b.java net/nitroshare/android/ui/explorer/Explorer Activity.java net/nitroshare/android/transfer/c.java net/nitroshare/android/transfer/e.java net/nitroshare/android/transfer/d.java net/nitroshare/android/transfer/d.java net/nitroshare/android/transfer/TransferSer vice.java
2	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/nitroshare/android/util/b.java net/nitroshare/android/ui/explorer/b.java net/nitroshare/android/ui/settings/b.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.

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 ['network connectivity'].
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 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 encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
--------	--------	-------------

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
nitroshare.net	ok	IP: 172.105.99.232 Country: Canada Region: Ontario City: Toronto Latitude: 43.700111 Longitude: -79.416298 View: Google Map
paolorotolo.github.io	ok	IP: 185.199.108.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map

HARDCODED SECRETS

POSSIBLE SECRETS

"library_appintro_authorWebsite" : "http://paolorotolo.github.io/"

POSSIBLE SECRETS

"library_appintro_authorWebsite": "http://paolorotolo.github.io/"

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.