MOBSF

ANDROID STATIC ANALYSIS REPORT

NitroShare (0.4.0.37)

File Name:	installer270.apk
Package Name:	net.nitroshare.android
Scan Date:	May 31, 2022, 8:25 a.m.
App Security Score:	60/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	6	1	1	1

FILE INFORMATION

File Name: installer270.apk
Size: 2.47MB
MD5: 7fcdf254d1c74890376593eaa1f05fa2
SHA1: cb0db3f3be1e5b28f4494be71f4f21fe7cc02eea
SHA256: 37662e4a39b8665f1178a21492757b0a64646164825e8d59f59b415182be835f

APP INFORMATION

App Name: NitroShare
Package Name: net.nitroshare.android
Main Activity: net.nitroshare.android.ui.transfer.TransferActivity
Target SDK: 27
Min SDK: 16
Max SDK:
Android Version Name: 0.4.0.37
Android Version Code: 38

APP COMPONENTS

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

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=Nathan Osman
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-05-18 06:06:26+00:00
Valid To: 2042-05-12 06:06:26+00:00
Issuer: CN=Nathan Osman
Serial Number: 0x4bf80a51
Hash Algorithm: sha256
md5: 08956f560c5b0a0d13992e9c491846d0
sha1: b7308f3673dbad16a3d73856e4deb139318f0b1a
sha256: 7a02b4892589e7d4840c8f509ee704d03c2459afd812d9c518a36b8eb7bada98
sha512: c2d8e85f6aa86bda7be4c60f30b25f076b14b609faca039a31d7747cd4b3e994906e154fda8298107b2fcc57e14297d8353c339a61da886fae0b3f4d672810e7
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: d8b66c5396ccfcab7d8d0668ede73318e55ab703416f1f433c488bcf25b702fc

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	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.

APKID ANALYSIS

FILE	DETAILS

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

NO	ISSUE	SEVERITY	DESCRIPTION
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	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/ui/explorer/b.java net/nitroshare/android/ui/settings/b.java net/nitroshare/android/util/b.java
2	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/nitroshare/android/ui/explorer/ExplorerActivity.java net/nitroshare/android/transfer/e.java com/b/a/ae.java net/nitroshare/android/transfer/c.java net/nitroshare/android/ui/ShareActivity.java com/github/paolorotolo/appintro/AppIntroBase.java net/nitroshare/android/transfer/d.java net/nitroshare/android/transfer/TransferService.java net/nitroshare/android/ui/transfer/b.java net/nitroshare/android/ui/transfer/TransferActivity.java android/a/b/i.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.
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.

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
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:** 185.199.109.153 **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.