

ANDROID STATIC ANALYSIS REPORT



NFCMessageBoard (3.2)

File Name:	installer29.apk
Package Name:	com.briankhuu.nfcmessageboard
Scan Date:	May 31, 2022, 7:38 a.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	♥ HOTSPOT
1	2	1	1	0

FILE INFORMATION

File Name: installer29.apk

Size: 1.04MB

MD5: 845936831a6b723d821225bdc2573885

SHA1: 0931c63f78b0468d2489f42aa2ac7a0653133c31

SHA256: 43f1930ddfe3588b5eeac9b7ee6d2ee1fa9f25a0d0d221539b683c006fe8595a

i APP INFORMATION

App Name: NFCMessageBoard

Package Name: com.briankhuu.nfcmessageboard

Main Activity: com.briankhuu.nfcmessageboard.MainScreen

Target SDK: 22 Min SDK: 10 Max SDK:

Android Version Name: 3.2 Android Version Code: 16

B APP COMPONENTS

Activities: 7 Services: 0 Receivers: 0 Providers: 0

Exported Activities: 1 Exported Services: 0 Exported Receivers: 0 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: 2015-04-06 07:18:53+00:00 Valid To: 2042-08-22 07:18:53+00:00

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

Serial Number: 0x4143a58d Hash Algorithm: sha256

md5: 370b9d4d4d80a2d34c4c084ed87fa251

sha1: e5f95cb2bd5f5b8276ef9f0d3400153aae566437

sha256: 229ea9f9afe1206df074005ce7e19101bef52e04e6a131dce3679fef53682070

sha512: 289c32e85a14cde6dbc3962f16126c67b7ee754cbca48598427eeca7539ba80d94639089b7633b1349331c29129fccacd2ea466dda29ea02dee1468f81e66562

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.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

M APKID ANALYSIS

FILE	DETAILS		
	FINDINGS	DETAILS	
classes.dex	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=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 (com.briankhuu.nfcmessageboard.ReadHtmlTags) 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.

</> 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/briankhuu/nfcmessageboard/WritingTo TextTag.java com/briankhuu/nfcmessageboard/ReadHtml Tags.java com/briankhuu/nfcmessageboard/TagDiagn ostics.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 ['NFC'].
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 no 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
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



POSSIBLE SECRETS

"preference_file_key": "com.briankhuu.nfcmessageboard.userpref"

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.