ANDROID STATIC ANALYSIS REPORT

Nounours and friends (3.4.4)

File Name:	installer3788.apk
Package Name:	ca.rmen.nounours
Scan Date:	May 31, 2022, 7:50 p.m.
App Security Score:	41/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	5	1	1	1

FILE INFORMATION

File Name: installer3788.apk
Size: 3.5MB
MD5: 47d8a34ed90df38858370ffd20188fef
SHA1: 520e7533d8b2dc1b1b4afbc116ec1dc400285d54
SHA256: c2ccb56412cabadbcfb980257fd28601293886505b968722d1700151265c238d

APP INFORMATION

App Name: Nounours and friends
Package Name: ca.rmen.nounours
Main Activity: ca.rmen.nounours.android.handheld.MainActivity
Target SDK: 25
Min SDK: 3
Max SDK:
Android Version Name: 3.4.4
Android Version Code: 344

APP COMPONENTS

Activities: 4
Services: 3
Receivers: 0
Providers: 0
Exported Activities: 2
Exported Services: 2
Exported Receivers: 0
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: 2015-10-12 13:54:18+00:00
Valid To: 2043-02-27 13:54:18+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x708e1d65
Hash Algorithm: sha256
md5: c19dd9a3490e82867adb03430e27f56c
sha1: 29284e779aa76f0e9bedf7b14414535a2bdad8a8
sha256: 6db36ef90a67f59d90377fbd7f3f2c909de3e7c67e433e4e7ec650168a345e65
sha512: 047ca1d89747d1bccace338adf9c71dec9982480b4d1552cbb7cc22658e343a69930d2893c9d9de088b33c983d8331559f3131ecf065c07ff34eb339163ea9ef
```

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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

APKID ANALYSIS

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

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	Activity (ca.rmen.nounours.android.handheld.settings.SettingsActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	Activity (ca.rmen.nounours.android.handheld.dream.DreamSettingsActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Service (ca.rmen.nounours.android.handheld.lwp.LWPService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_WALLPAPER [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Service (ca.rmen.nounours.android.handheld.dream.NounoursDreamService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_DREAM_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

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	ca/rmen/nounours/android/common/nounours/cache/SoundCache.java ca/rmen/nounours/android/handheld/nounours/orientation/SensorListener.java ca/rmen/nounours/android/handheld/MainActivity.java ca/rmen/nounours/android/handheld/nounours/SoundHandler.java ca/rmen/nounours/Util.java ca/rmen/nounours/io/ImageFeatureReader.java ca/rmen/nounours/android/common/nounours/cache/NounoursResourceCache.java ca/rmen/nounours/Nounours.java ca/rmen/nounours/android/handheld/compat/EnvironmentCompat.java ca/rmen/nounours/android/common/nounours/AndroidNounours.java ca/rmen/nounours/android/common/util/BitmapUtil.java ca/rmen/nounours/android/handheld/util/AnimationUtil.java ca/rmen/nounours/android/common/nounours/AnimationHandler.java ca/rmen/nounours/android/common/nounours/cache/ImageCache.java ca/rmen/nounours/android/handheld/AnimationSaveService.java ca/rmen/nounours/android/handheld/compat/NotificationCompat.java
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	ca/rmen/nounours/Nounours.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	ca/rmen/nounours/android/handheld/compat/Api8Helper.java ca/rmen/nounours/android/handheld/compat/EnvironmentCompat.java ca/rmen/nounours/android/handheld/util/FileUtil.java ca/rmen/nounours/android/handheld/util/AnimationUtil.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 use no 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 no hardware resources.
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 no 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	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.
9	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.

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
incompetech.com	ok	**IP:** 76.72.166.146 **Country:** United States of America **Region:** Pennsylvania **City:** Philadelphia **Latitude:** 39.962440 **Longitude:** -75.199928 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.jappit.com	ok	**IP:** 78.153.216.83 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

EMAILS

EMAIL	FILE
c@rmen.ca	Android String Resource

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.