

#### ANDROID STATIC ANALYSIS REPORT



**\$\Pi\$** GM Dice (0.1.5)

File Name:	installer265.apk
Package Name:	de.duenndns.gmdice
Scan Date:	May 31, 2022, 9:06 a.m.
App Security Score:	44/100 (MEDIUM RISK)
Grade:	

#### FINDINGS SEVERITY

<del>派</del> HIGH	▲ MEDIUM	<b>i</b> INFO	✓ SECURE	≪ HOTSPOT
2	2	1	1	0

#### FILE INFORMATION

File Name: installer265.apk

Size: 0.06MB

MD5: 585cd9c83211fc5d90680bd186b1d2e3

SHA1: f00a66398f5ae6f823d10bbbac61149498f13481

SHA256: 85f0ce211c84feb1418b799dd719a74707c3b45d0bb72a21a8828698ae28edcd

#### **i** APP INFORMATION

App Name: GM Dice

Package Name: de.duenndns.gmdice Main Activity: GameMasterDice

Target SDK: 8 Min SDK: 3 Max SDK:

Android Version Name: 0.1.5
Android Version Code: 6

#### **EE** APP COMPONENTS

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

Exported Activities: O Exported Services: O Exported Receivers: O Exported Providers: O



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: 2012-04-20 09:46:49+00:00 Valid To: 2039-09-06 09:46:49+00:00

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

Serial Number: 0x4f913089 Hash Algorithm: sha1

md5: 72f304e7b801e940fa6d144f993af805

sha1: 3b68f191a21bbe71821bf255c33382b4f5522454

sha256: a26b42202e9fed321295dd0be832a8fd8babaf875385f2e916b571633dff181e

sha512: 4edd718a69a2a1006296361559357b0d96299fec5e78f887f493e39ae79a42d027fab27bbaf1b22a9340aaf12156a11504059547181ac2b39a89e43352a99c52

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.	
Certificate algorithm might be vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.	

## **M** APKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS	DETAILS	
	Compiler	dx	

## **△** 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
1	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	de/duenndns/gmdice/GameMasterDic e.java de/duenndns/gmdice/DiceSet.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	de/duenndns/gmdice/GameMasterDic e.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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.
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 encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

# **Q DOMAIN MALWARE CHECK**

DOMAIN STATUS
---------------

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.gnu.org	ok	IP: 209.51.188.116 Country: United States of America Region: Massachusetts City: Boston Latitude: 42.358429 Longitude: -71.059769 View: Google Map



EMAIL	FILE
georg@op-co.de	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.

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