ANDROID STATIC ANALYSIS REPORT

No icon

Open Chaos Chess (1.6.4)

File Name:	installer164.apk
Package Name:	dev.corruptedark.openchaoschess
Scan Date:	May 30, 2022, 3:46 p.m.
App Security Score:	67/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	3	1	1	1

FILE INFORMATION

File Name: installer164.apk
Size: 1.06MB
MD5: 623920da0d8cb96675343e14c1be4cce
SHA1: 2ffffb98926d934e8bdbf1286b7b000a895ff043
SHA256: a830d708965e6f7ea8db2859b5485d9b798649ba55f611bcb559ae48205cd78f

APP INFORMATION

App Name: Open Chaos Chess
Package Name: dev.corruptedark.openchaoschess
Main Activity: dev.corruptedark.openchaoschess.MainActivity
Target SDK: 30
Min SDK: 16
Max SDK:
Android Version Name: 1.6.4
Android Version Code: 31

APP COMPONENTS

Activities: 10
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=US, ST=MI, L=Monroe, O=Corrupted Development, CN=Noah Stanford
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-11-18 17:21:35+00:00
Valid To: 2116-10-25 17:21:35+00:00
Issuer: C=US, ST=MI, L=Monroe, O=Corrupted Development, CN=Noah Stanford
Serial Number: 0x4ad118f8
Hash Algorithm: sha256
md5: 5252188be4204c022d6113e0b440697b
sha1: b2de452d8b7958b1283d21037f940c4dcd1ec1e8
sha256: 23c29df6d4666d3dbe313bc1f888aca8a01036c45ffa37cf7d123905507a6903
sha512: 355cef5a1080081544fdab4625fb4d89caaf7e04a916d98e896b8c6325768ee70be75ac83c56320e5c2ea71460841f637a077d29f65694c0c67512165d1f586a
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: a1730623696569a0aff860941409a0424f156a01461b380f4e977518fffcc68a
```

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.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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>Anti-VM Code</td><td>Build.FINGERPRINT check</td></tr>
<tr><td>Compiler</td><td>r8</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=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.

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	b/b/p/z0.java b/e/f/g.java b/b/p/y0.java b/b/o/f.java b/b/p/l0.java b/b/k/u.java b/h/a/e.java dev/corruptedark/openchaoschess/MultiPlayerBoard.java b/e/k/b.java b/b/p/w0.java b/e/k/w.java b/b/o/i/d.java b/b/p/c1.java b/b/p/t.java d/a/a/s.java d/a/a/m.java d/a/a/h.java b/b/k/k.java d/a/a/j.java b/b/p/j0.java b/m/a/a/g.java b/b/p/m0.java b/b/p/z.java d/a/a/t.java d/a/a/n.java b/e/f/c.java b/b/o/i/g.java b/e/f/l/d.java b/e/k/r.java dev/corruptedark/openchaoschess/StartHostActivity.java b/b/p/q0.java b/h/a/k.java b/e/f/d.java b/b/k/h.java b/e/j/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b/b/l/a/a.java b/b/p/v.java b/b/p/r0.java b/e/f/j.java b/e/f/e.java b/e/d/c.java b/e/d/b.java b/e/f/f.java d/a/a/k.java b/e/k/a.java b/f/a/b.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	dev/corruptedark/openchaoschess/MainActivity.java dev/corruptedark/openchaoschess/SinglePlayerBoard.java d/a/a/h.java c/a/a/a/a.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 ['bluetooth', 'location'].

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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	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
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

EMAILS

EMAIL	FILE
noahstandingford@gmail.com	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.