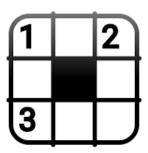


ANDROID STATIC ANALYSIS REPORT



Crossword (1.14)

File Name:	installer153.apk
Package Name:	org.billthefarmer.crossword
Scan Date:	May 31, 2022, 3:04 p.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

兼 HIGH	▲ MEDIUM	i INFO	✓ SECURE	ℚ HOTSPOT
1	1	0	1	0

FILE INFORMATION

File Name: installer153.apk

Size: 0.49MB

MD5: f1ea1203628e728747587e224f6efc16

SHA1: 076cbb3cd9f62c4c15552be477b08dd57ac1c12f

SHA256: c2c7e09712839f83ace407515d6c5cb978af5235a44385ff118a247a1c8c96f0

i APP INFORMATION

App Name: Crossword

Package Name: org.billthefarmer.crossword **Main Activity:** org.billthefarmer.crossword.Main

Target SDK: 28 Min SDK: 14 Max SDK:

Android Version Name: 1.14 Android Version Code: 114

EE APP COMPONENTS

Activities: 4 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: 2017-01-31 15:26:23+00:00 Valid To: 2044-06-18 15:26:23+00:00

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

Serial Number: 0x76108c71 Hash Algorithm: sha256

md5: 7c9f6728c829ab6a6e96a71b49bb495a

sha1: d01d2244a16e5aaec335121f78f618bae7b4636f

sha512: d4569b450ecd0cb20135d8cf04ae235366e4cefde47ca82bf63301feb53cba525c760f95fe08c27c32bd0f14b3fea4f05fb96788af2e46187861bcf6df79abf2

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.

M APKID ANALYSIS

FILE	DETAILS			
classes.dex	FINDINGS	DETAILS		
Classes.dex	Compiler	r8 without marker (suspicious)		

△ 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.

</> CODE ANALYSIS

					ı
NO	ISSUE	SEVERITY	STANDARDS	FILES	ì
					ı

■ 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
duckduckgo.com	ok	IP: 52.142.124.215 Country: Ireland Region: Dublin City: Dublin Latitude: 53.343990 Longitude: -6.267190 View: Google Map

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.