

ANDROID STATIC ANALYSIS REPORT



Werewolf (1.0)

File Name:	installer3798.apk
Package Name:	org.secuso.privacyfriendlycardgameone
Scan Date:	May 31, 2022, 7:18 p.m.
App Security Score:	60/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	♥ HOTSPOT
1	6	1	2	0

FILE INFORMATION

File Name: installer3798.apk

Size: 8.25MB

MD5: 29eebdc841443d969642fcf7bbf32a18

SHA1: d81c60d4f0478a25d17b884cfbae04cacd7f47c1

SHA256: e0c39c67ef83bff8f48f528577faa2d4e6aff43b147d01071361641ec3b939be

i APP INFORMATION

App Name: Werewolf

Package Name: org.secuso.privacyfriendlycardgameone

 ${\it Main\ Activity:} or g. secuso. privacy friendly we rwolf. activity. Splash Activity$

Target SDK: 25 Min SDK: 21 Max SDK:

Android Version Name: 1.0
Android Version Code: 1

EE APP COMPONENTS

Activities: 9 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: 2018-05-18 05:55:02+00:00 Valid To: 2045-10-03 05:55:02+00:00

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

Serial Number: 0x473b5fb2 Hash Algorithm: sha256

md5: 39e91999d07fce78d21a38fa279e0df3

sha1: c0093efb74242aa042beb0e382153febaf962b43

sha256: ad0d486e8c9abffcb00df11b30c9e43e1cfcaad7cd6038ccb54a84c8ebf5ed63

sha512: 4f89db09eb6ed4c1884e38a6263d00a3fe291d74a70daf8e59bbb8841fa064b439c99b1b575ad7902e8ae4842f9da2705d6abf6dac10be4eb0da31afb4306c67

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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

M APKID ANALYSIS

FILE	DETAILS				
	FINDINGS	DETAILS			
classes.dex	Compiler	dx (possible dexmerge)			
	Manipulator Found	dexmerge			



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

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	org/secuso/privacyfriendlywerwolf/client/Webso cketClientHandler.java org/secuso/privacyfriendlywerwolf/server/WebS ocketServerHandler.java com/koushikdutta/async/PushParser.java com/koushikdutta/async/Util.java org/secuso/privacyfriendlywerwolf/dialog/Witch Dialog.java org/secuso/privacyfriendlywerwolf/activity/Game Activity.java com/koushikdutta/async/AsyncServer.java org/secuso/privacyfriendlywerwolf/client/ClientG ameController.java com/koushikdutta/async/AsyncNetworkSocket.ja va org/secuso/privacyfriendlywerwolf/helpers/Playe rCardClickListener.java com/koushikdutta/async/http/HybiParser.java org/secuso/privacyfriendlywerwolf/server/Server GameController.java org/secuso/privacyfriendlywerwolf/context/Gam eContext.java com/koushikdutta/async/ByteBufferList.java org/secuso/privacyfriendlywerwolf/server/Voting Controller.java com/koushikdutta/async/http/cache/RawHeaders .java org/secuso/privacyfriendlywerwolf/dialog/Voting Dialog.java com/koushikdutta/async/http/AsyncHttpRequest.java org/secuso/privacyfriendlywerwolf/dialog/Voting Dialog.java com/koushikdutta/async/http/AsyncHttpRequest.java org/secuso/privacyfriendlywerwolf/util/GameUtil.java com/koushikdutta/async/http/server/AsyncHttpS erverRequestImpl.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/koushikdutta/async/dns/Dns.java com/koushikdutta/async/AsyncSSLSocketWrappe r.java
3	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	com/koushikdutta/async/dns/Dns.java org/secuso/privacyfriendlywerwolf/server/Server GameController.java com/koushikdutta/async/util/FileCache.java
4	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/koushikdutta/async/http/spdy/ByteString.ja va
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/koushikdutta/async/AsyncSSLSocketWrappe r.java
6	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/koushikdutta/async/http/WebSocketImpl.jav a

■ 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 ['network connectivity'].
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 user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
11	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
12	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
13	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The certificate path must terminate with a trusted CA certificate'].
14	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.

₽ HARDCODED SECRETS

POSSIBLE SECRETS "about_author": "Authors:" "about_author": "Autoren:"

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.