MobSF

ANDROID STATIC ANALYSIS REPORT

🤖 Werewolf (1.0.1)

File Name:	installer3817.apk
Package Name:	org.secuso.privacyfriendlycardgameone
Scan Date:	May 31, 2022, 5:46 p.m.
App Security Score:	**60/100 (LOW RISK)**
Grade:	A

⬤ FINDINGS SEVERITY

🐞 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
1	6	1	2	0

📦 FILE INFORMATION

File Name: installer3817.apk
Size: 8.04MB
MD5: aad31df44fca607ba97ee910ad6204e0
SHA1: c6ad24bfaa53769d4b5ce1ab14d068681b1738d8
SHA256: 63a898a1880cc20e9a63d78c6acbc0c3fe24ef78361d2925213642be31a45ed0

ℹ APP INFORMATION

App Name: Werewolf
Package Name: org.secuso.privacyfriendlycardgameone
Main Activity: org.secuso.privacyfriendlywerwolf.activity.SplashActivity
Target SDK: 25
Min SDK: 21
Max SDK:
Android Version Name: 1.0.1
Android Version Code: 2

■■ APP COMPONENTS

Activities: 9
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: False
v3 signature: False
Found 1 unique certificates
Subject: CN=Philipp Rack
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-09-10 20:08:38+00:00
Valid To: 2064-08-28 20:08:38+00:00
Issuer: CN=Philipp Rack
Serial Number: 0x7e8ad4ee
Hash Algorithm: sha256
md5: 19e202e493d8f3457c4d644384f6de47
sha1: ce01a61218b97ac4deaa75da4e5afbda059dff20
sha256: 466d66dc058f73043e5e9bdd5606fdaec19d8f80c47f44c1807d65775d735c3f
sha512: 19c5e7d279047057951b490b305c5aa806be70cfc4dbac3130bd34b37b450da982bc1645c9e769b4c8e56e7d4a085ac34bd83b138e5090b9ba0e4516dbcd4976

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.

🔍 APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><td>FINDINGS</td><td>DETAILS</td></tr><tr><td>Compiler</td><td>r8</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

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/activity/GameActivity.java com/koushikdutta/async/http/server/AsyncHttpServerRequestImpl.java com/koushikdutta/async/http/AsyncHttpRequest.java org/secuso/privacyfriendlywerwolf/helpers/PlayerCardClickListener.java org/secuso/privacyfriendlywerwolf/server/WebSocketServerHandler.java org/secuso/privacyfriendlywerwolf/util/GameUtil.java org/secuso/privacyfriendlywerwolf/context/GameContext.java org/secuso/privacyfriendlywerwolf/dialog/WitchDialog.java org/secuso/privacyfriendlywerwolf/client/ClientGameController.java com/koushikdutta/async/PushParser.java org/secuso/privacyfriendlywerwolf/server/VotingController.java com/koushikdutta/async/AsyncServer.java com/koushikdutta/async/http/HybiParser.java com/koushikdutta/async/AsyncNetworkSocket.java org/secuso/privacyfriendlywerwolf/server/ServerGameController.java org/secuso/privacyfriendlywerwolf/dialog/VotingDialog.java com/koushikdutta/async/ByteBufferList.java org/secuso/privacyfriendlywerwolf/client/WebsocketClientHandler.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/koushikdutta/async/AsyncSSLSocketWrapper.java com/koushikdutta/async/dns/Dns.java
4	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/AsyncSSLSocketWrapper.java
5	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	org/secuso/privacyfriendlywerwolf/dialog/PlayerInputDialog.java com/koushikdutta/async/util/FileCache.java com/koushikdutta/async/dns/Dns.java org/secuso/privacyfriendlywerwolf/server/ServerGameController.java org/secuso/privacyfriendlywerwolf/activity/StartClientActivity.java
6	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.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 ['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.