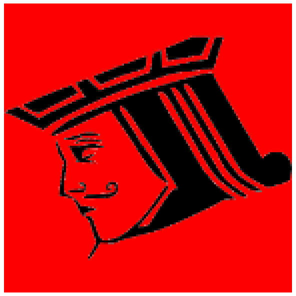
ANDROID STATIC ANALYSIS REPORT



Vitosha Blackjack (2.0.0)

File Name:	installer3770.apk
Package Name:	eu.veldsoft.vitosha.blackjack
Scan Date:	May 31, 2022, 7:08 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	2	1	1	0

FILE INFORMATION

File Name: installer3770.apk
Size: 1.54MB
MD5: 8f058e34f338c00960c4e53f76142fe2
SHA1: a27932fe591461199eb6162f1319b7b19f769572
SHA256: 87bf55d4eab43c7f2b0c0fd5e15f9adb69adec90aac33397f7c97637cdad7184

APP INFORMATION

App Name: Vitosha Blackjack
Package Name: eu.veldsoft.vitosha.blackjack
Main Activity: eu.veldsoft.vitosha.blackjack.SplashActivity
Target SDK: 23
Min SDK: 15
Max SDK:
Android Version Name: 2.0.0
Android Version Code: 2

APP COMPONENTS

Activities: 6
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: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-05-02 08:15:33+00:00
Valid To: 2046-09-17 08:15:33+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x4d706254
Hash Algorithm: sha256
md5: 52ebf23a41f38ddf41780c20b473bd53
sha1: 82017e2d181c4edbf9e4c7355f978537cb1399f8
sha256: a679aefa61d58a3d8f67c31f41b4d93e9ee3d2955d31f52f2f490e3bd0b9ebad
sha512: 41629aa6c9eea1dddd14dc93d8f465058c3a903b6327618e7e238c000f6909dd786b1fc54884124e46526928cc06985f6404a8a3d2a41564bbb8a11254c95a2e
```

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.

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>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	eu/veldsoft/vitosha/blackjack/Dealer.java org/encog/util/simple/EncogUtility.java org/encog/plugin/system/SystemLoggingPlugin.java org/encog/ensemble/aggregator/MetaClassifier.java org/encog/Test.java org/encog/ensemble/GenericEnsembleML.java org/encog/neural/prune/PruneIncremental.java org/encog/mathutil/libsvm/svm.java org/encog/ensemble/Ensemble.java org/encog/ml/world/basic/BasicAgent.java org/encog/util/text/DoubleString.java eu/veldsoft/vitosha/blackjack/Deck.java org/encog/app/analyst/ConsoleAnalystListener.java
				org/encog/ml/prg/generator/RampedHalfAndHalf.java org/encog/ml/genetic/crossover/SpliceNoRepeat.java org/encog/neural/hyperneat/HyperNEATGenome.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	org/encog/ml/prg/opp/SubtreeMutation.java org/encog/neural/neat/NEATGenomeFactory.java org/encog/ml/prg/extension/BasicTemplate.java org/encog/ensemble/data/factories/WeightedResamplingDataSetFactory.java org/encog/ml/prg/opp/ConstMutation.java org/encog/mathutil/randomize/generate/SecureGenerateRandom.java org/encog/mathutil/VectorAlgebra.java org/encog/ml/ea/population/PopulationGenerator.java org/encog/mathutil/randomize/generate/BasicGenerateRandom.java org/encog/ml/ea/opp/selection/TournamentSelection.java org/encog/mathutil/randomize/factory/RandomFactory.java org/encog/neural/neat/training/opp/NEATMutateAddNode.java org/encog/neural/neat/training/opp/links/SelectFixed.java org/encog/neural/neat/NEATPopulation.java org/encog/neural/neat/training/opp/links/SelectLinks.java org/encog/ml/prg/extension/StandardExtensions.java org/encog/ml/prg/generator/AbstractGenerator.java org/encog/neural/neat/training/opp/NEATCrossover.java org/encog/mathutil/randomize/factory/BasicRandomFactory.java org/encog/ml/genetic/crossover/Splice.java org/encog/util/http/FormUtility.java org/encog/mathutil/randomize/RandomChoice.java org/encog/ml/genetic/mutate/MutateShuffle.java org/encog/ml/prg/opp/SubtreeCrossover.java org/encog/ml/ea/opp/EvolutionaryOperator.java org/encog/ml/prg/EncogProgram.java org/encog/Test.java org/encog/ml/ea/opp/selection/TruncationSelection.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/encog/util/obj/ChooseObject.java org/encog/neural/neat/FactorNEATGenome.java org/encog/ensemble/data/factories/ResamplingDataSetFactory.java org/encog/mathutil/libsvm/svm.java org/encog/ml/prg/generator/PrgGrowGenerator.java org/encog/neural/neat/training/opp/links/MutatePerturbLinkWeight.java org/encog/ml/hmm/distributions/ContinousDistribution.java org/encog/ml/prg/generator/GenerateWorker.java org/encog/app/analyst/commands/CmdCreate.java org/encog/ml/prg/generator/PrgGenerator.java org/encog/neural/neat/training/opp/links/SelectProportion.java org/encog/ml/genetic/mutate/MutatePerturb.java org/encog/neural/neat/training/opp/links/MutateLinkWeight.java org/encog/ml/ea/opp/OperationList.java org/encog/neural/neat/training/opp/NEATMutateRemoveLink.java org/encog/neural/hyperneat/FactorHyperNEATGenome.java org/encog/neural/neat/training/opp/links/MutateResetLinkWeight.java org/encog/ml/ea/opp/CompoundOperator.java org/encog/ml/factory/method/EPLFactory.java org/encog/ml/ea/opp/selection/SelectionOperator.java org/encog/neural/neat/training/opp/NEATMutateAddLink.java org/encog/mathutil/randomize/RangeRandomizer.java org/encog/ml/prg/generator/PrgFullGenerator.java org/encog/neural/neat/training/opp/NEATMutateWeights.java org/encog/neural/neat/training/NEATGenome.java org/encog/ml/ea/train/basic/EAWorker.java org/encog/ml/prg/extension/ProgramExtensionTem

NO	ISSUE	SEVERITY	STANDARDS	FILES
				plate.java org/encog/ml/prg/generator/AbstractPrgGenerator.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 invoke platform-provided 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
search.yahooapis.com	ok	No Geolocation information available.
schemas.openxmlformats.org	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.heatonresearch.com	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ichart.finance.yahoo.com	ok	No Geolocation information available.
developer.android.com	ok	**IP:** 142.250.179.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
docs.oracle.com	ok	**IP:** 23.222.34.164 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **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.