

ANDROID STATIC ANALYSIS REPORT

TU

Mensa-Guthaben (1.1.2)

File Name:	installer259.apk
Package Name:	de.yazo_games.mensaguthaben
Scan Date:	May 31, 2022, 9:06 a.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

兼 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
1	2	1	1	0

FILE INFORMATION

File Name: installer259.apk

Size: 0.42MB

MD5: a52e5f0450f5fd6b508ad6f01ffed8bc

SHA1: 781f159d87f6dbd6a9dac7842fef11e60feb00c8

SHA256: 578fee2677d44906b9439cd50b0e985de2414b7e5c98bf546c13ea47bf790683

i APP INFORMATION

App Name: Mensa-Guthaben

Package Name: de.yazo_games.mensaguthaben

Main Activity: de.yazo_games.mensaguthaben.MainActivity

Target SDK: 19 Min SDK: 11 Max SDK:

Android Version Name: 1.1.2
Android Version Code: 13

B APP COMPONENTS

Activities: 3 Services: 0 Receivers: 0 Providers: 0

Exported Activities: 1 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: 2014-11-04 06:15:25+00:00 Valid To: 2042-03-22 06:15:25+00:00

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

Serial Number: 0x3f2c3171 Hash Algorithm: sha256

md5: da8d66d0c732abe2d6f6205f446ffe0b

sha1: b80b2aee7c174651fbd889e091e13492162ebd6c

sha256: 794b5a5716ea981a345f144966ba5cdca1f669394b5324691fc0af7df5442856

sha512: e720a75b6671566fd680216b7c07aa2b0e1c06804b8b2bdd029599e45fd8039d4c8c1f1777a30d5cf6f0775cb55aa2a54584de40630ca6a13e1aaf5823ac9ec7

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.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.

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.
2	Activity-Alias (de.yazo_games.mensaguthaben.ActivityAlias) is not Protected. An intent-filter exists.	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity-Alias is explicitly exported.

</> 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	de/yazo_games/mensaguthaben/AutostartRegiste r.java de/yazo_games/mensaguthaben/cardreader/Mag naCartaReader.java com/codebutler/farebot/Utils.java de/yazo_games/mensaguthaben/MainActivity.jav a de/yazo_games/mensaguthaben/cardreader/Rea ders.java de/yazo_games/mensaguthaben/cardreader/Inter cardReader.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 ['NFC'].
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	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 not encrypt any data in traffic or does not transmit any data between itself and another trusted IT product.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
xml.apache.org	ok	IP: 151.101.2.132 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 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 | $\underline{\mbox{Ajin Abraham}}$ | $\underline{\mbox{OpenSecurity}}.$