MOBSF

ANDROID STATIC ANALYSIS REPORT

MHGU Database (2.3.6)

File Name:	installer3762.apk
Package Name:	com.ghstudios.android.mhgendatabase
Scan Date:	May 31, 2022, 7:36 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	3	2	1	0

FILE INFORMATION

File Name: installer3762.apk
Size: 8.85MB
MD5: 1a44d5f5d191e873c50389f78639d284
SHA1: a67fe79c4403dbe9aea9518deadafae1cde6b103
SHA256: 48bb2e6f00521d0b3a29f229caaeb3378d066fb94f04efc057b59b401f35a7f5

APP INFORMATION

App Name: MHGU Database
Package Name: com.ghstudios.android.mhgendatabase
Main Activity: com.ghstudios.android.features.monsters.list.MonsterListPagerActivity
Target SDK: 27
Min SDK: 14
Max SDK:
Android Version Name: 2.3.6
Android Version Code: 21

APP COMPONENTS

Activities: 31
Services: 0
Receivers: 0
Providers: 1
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: 2016-08-18 08:58:26+00:00
Valid To: 2044-01-04 08:58:26+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0xd4cad5d
Hash Algorithm: sha256
md5: 6712d2737b0daece6863217794cd64ab
sha1: fb71de12988f4d3913920917df8d346ebd116bec
sha256: a70cbade678aaf8936416a344e90d425d371777ca12da0faad0559dc056980eb
sha512: d58c7d9004dfac36eb70d74f618957e92d6562c87cb52bdddbbf57fc120e55647ac4d58fab6d55373b0bb9aa4d7e449f9dfb56cdb910d640221aa17d364b1cf5

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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: DETAILS Compiler: dx

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION

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
				com/ghstudios/android/features/wishlist/external/b.java com/ghstudios/android/features/monsters/detail/MonsterSummaryFragment.java com/ghstudios/android/features/wishlist/detail/WishlistDetailViewModel.java com/ghstudios/android/features/armor/list/ArmorFamilyListViewModel.java com/ghstudios/android/features/skills/detail/SkillDetailViewModel.java com/ghstudios/android/features/search/UniversalSearchViewModel.java com/ghstudios/android/features/armorsetbuilder/detail/ASBDetailViewModel.java com/ghstudios/android/o.java com/ghstudios/android/k.java com/ghstudios/android/features/armorsetbuilder/armorselect/ArmorSelectViewModel.java a/a/a/a/a.java com/ghstudios/android/features/quests/QuestDetailViewModel.java com/d/a/a.java com/ghstudios/android/features/armor/detail/ArmorDetailViewModel.java

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	com/ghstudios/android/features/monsters/detail/e.java com/ghstudios/android/features/weapons/detail/e.java com/ghstudios/android/c/b.java com/a/a/a/a/a.java com/d/a/b.java com/ghstudios/android/features/wishlist/external/WishlistAddItemViewModel.java com/ghstudios/android/features/palicos/PalicoArmorListViewModel.java com/ghstudios/android/i.java com/ghstudios/android/features/weapons/detail/WeaponDetailViewModel.java com/d/a/c.java com/ghstudios/android/c/a/a.java com/ghstudios/android/features/armorsetbuilder/a.java com/ghstudios/android/c/a/l.java com/ghstudios/android/c.java com/ghstudios/android/features/items/detail/ItemDetailViewModel.java com/ghstudios/android/features/monsters/list/MonsterListViewModel.java com/ghstudios/android/features/wishlist/detail/a.java com/ghstudios/android/c/a/aq.java com/ghstudios/android/features/decorations/detail/DecorationDetailViewModel.java com/ghstudios/android/features/armor/detail/ArmorSetDetailViewModel.java com/ghstudios/android/c/a.java com/ghstudios/android/features/wishlist/list/WishlistListViewModel.java com/ghstudios/android/features/monsters/detail/MonsterDetailViewModel.java butterknife/ButterKnife.java com/ghstudios/android/c/c/f.java com/ghstudios/android/features/monsters/detail/b.java com/ghstudios/android/features/armorsetb

NO	ISSUE	SEVERITY	STANDARDS	FILES
				uilder/detail/ASBDetailPagerActivity.java com/ghstudios/android/features/armorsetbuilder/talismans/ASBTalismanListViewModel.java com/ghstudios/android/features/search/UniversalSearchActivity.java
2	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/ghstudios/android/a.java com/ghstudios/android/c/c/f.java
3	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/d/a/a.java com/ghstudios/android/c/c/b.java com/ghstudios/android/c/c/e.java com/ghstudios/android/c/c/c.java com/ghstudios/android/c/c/g.java com/ghstudios/android/c/c/d.java com/ghstudios/android/c/c/a.java com/ghstudios/android/c/c/f.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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to no hardware resources.
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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
cketti.de	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
xmlpull.org	ok	**IP:** 74.50.61.58 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.814899 **Longitude:** -96.879204 **View:** Google Map

EMAILS

EMAIL	FILE
contact@gatheringhallstudios.com	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"key" : "Key"
"library_ckChangeLog_author" : "cketti"
"library_ckChangeLog_authorWebsite" : "http://cketti.de/"
"key" : "Clave"
"key" : "Key"

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.