ANDROID STATIC ANALYSIS REPORT

MHGU Database (2.4.0)

File Name:	installer3786.apk
Package Name:	com.ghstudios.android.mhgendatabase
Scan Date:	May 31, 2022, 5:40 p.m.
App Security Score:	64/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
0	4	2	1	0

FILE INFORMATION

File Name: installer3786.apk
Size: 8.81MB
MD5: 9be784c1b8b6d7d062cd925dd9d11702
SHA1: f3e39ef2c32c50e1bb1ebd56e89ef0efc3673d60
SHA256: ffd260175cd9cf967ce95266bf3adaabe0defe774462c5a897ad17fa8484b6ab

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: 2.4.0
Android Version Code: 22

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: True
v3 signature: False
Found 1 unique certificates
Subject: ST=Ky, L=Louisville, O=Gathering Hall Studios, OU=Organization, CN=Gathering Hall
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-07-14 13:07:33+00:00
Valid To: 2041-07-08 13:07:33+00:00
Issuer: ST=Ky, L=Louisville, O=Gathering Hall Studios, OU=Organization, CN=Gathering Hall
Serial Number: 0x143f3107
Hash Algorithm: sha256
md5: cb16884b3eccefca73785035bc35b38d
sha1: 726bf53770159af28113d675192667ce3cc5de58
sha256: f4f81a09389f8818498e477a05dfae0893f9f22ec4f6ee1588634ede36cdde0b
sha512: 5899e59d3fd575df08854b4730599fd8bc91740b4087478830165fc3e8e3db56d4a31b6361f5544f5ecc8b68d8f7f06833be7ece749f65b60971e3430a6b3d7f
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 0aa9bdc062fc20858b29dadb9c9e98f6f8edf7f951a385d1db50580de7cf2d92
```

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	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

<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>dx</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	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/ghstudios/android/c/c/a.java com/d/a/a.java com/ghstudios/android/c/c/f.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/d/a/a.java com/ghstudios/android/features/weapons/detail/WeaponDetailViewModel.java com/ghstudios/android/features/armorsetbuilder/talismans/ASBTalismanListViewModel.java com/ghstudios/android/c/a/aq.java com/ghstudios/android/c/c/f.java com/ghstudios/android/features/palicos/PalicoArmorListViewModel.java com/ghstudios/android/features/wishlist/detail/a.java com/ghstudios/android/c/b.java com/ghstudios/android/features/decorations/detail/DecorationDetailViewModel.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/d/a/b.java com/ghstudios/android/features/monsters/list/MonsterListViewModel.java com/ghstudios/android/features/armorsetbuilder/detail/ASBDetailViewModel.java com/ghstudios/android/features/armor/detail/ArmorSetDetailViewModel.java com/ghstudios/android/features/wishlist/list/WishlistListViewModel.java com/ghstudios/android/features/armorsetbuilder/a.java butterknife/ButterKnife.java com/ghstudios/android/k.java com/ghstudios/android/features/wishlist/external/b.java com/ghstudios/android/features/armorsetbuilder/detail/ASBDetailPagerActivity.java com/ghstudios/android/features/monsters/detail/MonsterDetailViewModel.java com/ghstudios/android/i.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/monsters/detail/b.java com/ghstudios/android/features/search/UniversalSearchActivity.java a/a/a/a/a.java com/ghstudios/android/features/monsters/detail/e.java com/ghstudios/android/features/monsters/detail/MonsterSummaryFragment.java com/ghstudios/android/features/search/UniversalSearchViewModel.java com/ghstudios/android/o.java com/a/a/a/a/a.java com/d/a/c.java com/ghstudios/android/features/armor/deta

NO	ISSUE	SEVERITY	STANDARDS	FILES
				il/ArmorDetailViewModel.java com/ghstudios/android/features/armorsetbuilder/armorselect/ArmorSelectViewModel.java com/ghstudios/android/features/weapons/detail/e.java com/ghstudios/android/features/items/detail/ItemDetailViewModel.java com/ghstudios/android/features/quests/QuestDetailViewModel.java com/ghstudios/android/c.java com/ghstudios/android/features/wishlist/external/WishlistAddItemViewModel.java com/ghstudios/android/c/a/a.java com/ghstudios/android/c/a/l.java com/ghstudios/android/c/a.java
3	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/c/c/f.java com/ghstudios/android/a.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.