

#### ANDROID STATIC ANALYSIS REPORT



MHGU Database (2.1.1)

File Name:	installer3787.apk
Package Name:	com.ghstudios.android.mhgendatabase
Scan Date:	May 31, 2022, 5:50 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	

#### FINDINGS SEVERITY

<del>派</del> HIGH	▲ MEDIUM	<b>i</b> INFO	✓ SECURE	≪ HOTSPOT
1	3	2	1	0

#### FILE INFORMATION

File Name: installer3787.apk

Size: 8.36MB

MD5: a7902e11aa97480f34456278d47e72ca

SHA1: c24734797372651b8086aeb34d8fa0287df039e4

SHA256: 36a00f8f000865a8d91a34889c0e5712133048909112a2af0512a1c6afa40977

#### **i** APP INFORMATION

App Name: MHGU Database

Package Name: com.ghstudios.android.mhgendatabase

 $\textbf{\textit{Main Activity}:} com.ghstudios.and roid.features.monsters.list. Monster List Pager Activity$ 

Target SDK: 27 Min SDK: 14 Max SDK:

Android Version Name: 2.1.1 Android Version Code: 12

#### **EE** APP COMPONENTS

Activities: 30 Services: 0 Receivers: 0 Providers: 1

Exported Activities: O Exported Services: O Exported Receivers: O Exported Providers: O



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: a70cbade 678 aaf 8936416 a344 e90d425d371777 ca12da0 faad 0559dc 056980 ebad 25d371777 ca12da0 faad 0559dc 056980 ebad 25d37177 ca12da0 faad 056980 ebad 25d37177 ca12da0 faad 056980 ebad 25d3717 ca12da0 ebad 25d3717 ca12

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.

# **M** APKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS DETAILS		
Classes.uex	Compiler	dx	

### **△** NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

## **Q** 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/j.java com/ghstudios/android/features/decoration s/detail/DecorationDetailViewModel.java com/ghstudios/android/features/armorsetb uilder/a.java butterknife/ButterKnife.java com/ghstudios/android/features/monsters/ detail/MonsterDetailViewModel.java com/ghstudios/android/features/armorsetb uilder/detail/f.java com/ghstudios/android/c/a/ap.java com/ghstudios/android/features/wishlist/ex ternal/b.java com/ghstudios/android/features/weapons/ detail/WeaponDetailViewModel.java com/ghstudios/android/features/search/Uni versalSearchActivity.java com/ghstudios/android/features/monsters/ detail/MonsterSummaryFragment.java com/ghstudios/android/features/items/deta il/ItemDetailViewModel.java com/ghstudios/android/features/items/deta il/ItemDetailViewModel.java com/ghstudios/android/c/b.java com/ghstudios/android/c/b.java com/ghstudios/android/features/search/Uni

NO	ISSUE The Applogs information, Sensitive	SEVERITY	STANDARDS CWE: CWE-532: Insertion of Sensitive	versalSearchViewModel.java  Tologopo
	information should never be logged.	info	Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/ghstudios/android/features/quests/Qu estDetailViewModel.java com/ghstudios/android/features/monsters/ detail/h.java com/ghstudios/android/features/wishlist/de tail/a.java com/ghstudios/android/c/a/a.java com/ghstudios/android/features/armorsetb uilder/detail/ASBDetailViewModel.java com/ghstudios/android/features/armorsetb uilder/detail/ASBPagerActivity.java com/ghstudios/android/features/wishlist/ex ternal/WishlistAddItemViewModel.java com/a/a/a/a.java com/ghstudios/android/features/armorsetb uilder/armorselect/ArmorSelectViewModel.java com/ghstudios/android/features/armorsetb uilder/armorselect/ArmorSelectViewModel.java com/ghstudios/android/h.java com/ghstudios/android/features/palicos/Pal icoArmorListViewModel.java com/ghstudios/android/features/monsters/l ist/MonsterListViewModel.java com/ghstudios/android/features/monsters/l ist/MonsterListViewModel.java com/ghstudios/android/features/armor/det ail/ArmorSetDetailViewModel.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/d.java com/ghstudios/android/c/c/h.java com/ghstudios/android/c/c/a.java com/ghstudios/android/c/c/f.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/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.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to no hardware resources.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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
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

DOMAIN	STATUS	GEOLOCATION
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



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

#### 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.