MOBSF

ANDROID STATIC ANALYSIS REPORT

MHWorld Database (2.0.0)

File Name:	installer131.apk
Package Name:	com.gatheringhallstudios.mhworlddatabase
Scan Date:	May 31, 2022, 12:10 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: installer131.apk
Size: 20.61MB
MD5: a5ce2814d6870e706329cd1f3450f602
SHA1: 5c75f72c91d79cc4c01ea5493fcf4c5b43728144
SHA256: aa9bd12a691a00e1c7c0ddb7ae4bf8ff1c97b10ea2baecce64c19f1fa2635a41

APP INFORMATION

App Name: MHWorld Database
Package Name: com.gatheringhallstudios.mhworlddatabase
Main Activity: com.gatheringhallstudios.mhworlddatabase.SplashActivity
Target SDK: 28
Min SDK: 19
Max SDK:
Android Version Name: 2.0.0
Android Version Code: 21

APP COMPONENTS

Activities: 4
Services: 1
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: 2020-08-31 07:31:11+00:00
Valid To: 2048-01-17 07:31:11+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x1a4011ab
Hash Algorithm: sha256
md5: a85d5ec93d30deab3726cd4772f4a42c
sha1: ad0906ac97667e2afc54cd92dae3224269f04923
sha256: bad5cb3deb0cbbd35913f73fedbc9258b2574f164707de8950ac77def4fccb8d
sha512: c2006294664271836ea4db3741b6661a5b28cb9913beb1ae39cae2a8e558dcc4af697aa04ab2d17ac172702f61239cc77b4765680574da5692804b06266d9204

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 Anti-VM Code: Build.MANUFACTURER check Compiler: r8

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	butterknife/ButterKnife.java com/gatheringhallstudios/mhworlddatabase/components/SkillLevelView.java com/gatheringhallstudios/mhworlddatabase/assets/AssetExtensionsKt.java com/gatheringhallstudios/mhworlddatabase/util/pager/GenericPagerAdapter.java com/gatheringhallstudios/mhworlddatabase/util/Functions$loggedThread$1.java com/gatheringhallstudios/mhworlddatabase/assets/ColoredVectorDrawable$basePath$2.java com/michaelflisar/changelog/internal/ChangelogParserAsyncTask.java com/michaelflisar/changelog/internal/ParcelUtil.java com/gatheringhallstudios/mhworlddatabase/features/weapons/WeaponTreeAdapter.java com/michaelflisar/changelog/ChangelogParserUtil.java com/gatheringhallstudios/mhworlddatabase/components/HeaderItemDivider.java com/gatheringhallstudios/mhworlddatabase/util/pager/BasePagerFragment.java com/sdsmdg/harjot/vectormaster/utilities/legacyparser/PathParser.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
			OWASP MASVS: MSTG-STORAGE-3	com/michaelflisar/changelog/ChangelogBuilder.java com/gatheringhallstudios/mhworlddatabase/util/Functions$createLiveData$$inlined$loggedThread$1.java com/gatheringhallstudios/mhworlddatabase/features/workshop/selectors/WorkshopSelectorViewModel.java com/sdsmdg/harjot/vectormaster/utilities/parser/PathParser.java com/gatheringhallstudios/mhworlddatabase/util/sqliteloader/sqliteasset/Utils.java com/gatheringhallstudios/mhworlddatabase/data/AppConverters.java com/gatheringhallstudios/mhworlddatabase/features/kinsects/KinsectTreeAdapter.java com/gatheringhallstudios/mhworlddatabase/util/sqliteloader/sqliteasset/VersionComparator.java com/gatheringhallstudios/mhworlddatabase/util/sqliteloader/sqliteasset/SQLiteAssetHelper.java com/gatheringhallstudios/mhworlddatabase/features/search/UniversalSearchViewModel.java
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/gatheringhallstudios/mhworlddatabase/util/sqliteloader/adapters/FrameworkSQLiteDatabase.java com/gatheringhallstudios/mhworlddatabase/util/sqliteloader/sqliteasset/SQLiteAssetHelper.java
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/gatheringhallstudios/mhworlddatabase/data/dao/SkillDao.java com/michaelflisar/changelog/internal/ChangelogPreferenceUtil.java com/gatheringhallstudios/mhworlddatabase/data/entities/SkillTreeEntity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/gatheringhallstudios/mhworlddatabase/AppSettings.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.
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 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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.251.36.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
contact@gatheringhallstudios.com	Android String Resource

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.