# ANDROID STATIC ANALYSIS REPORT

## MHWorld Database (2.1.0)

| | |
|---|---|
| File Name: | installer281.apk |
| Package Name: | com.gatheringhallstudios.mhworlddatabase |
| Scan Date: | May 31, 2022, 1:06 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:** installer281.apk
**Size:** 21.3MB
**MD5:** 094f944d2d0ecf67ce704add57dd754f
**SHA1:** a80a8c0600ff7260f3a8b2af92fa300b5fc322f5
**SHA256:** ba90c7e565afc8ce5f742f2ca31cb6be93a08934b79cd326c70ced820da2f811

# 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:** 2.1.0
**Android Version Code:** 22

# 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: 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>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8</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 | The App logs information. Sensitive information should never be logged. | info | CWE: CWE-532: Insertion of Sensitive Information into Log File<br>OWASP MASVS: MSTG-STORAGE-3 | com/sdsmdg/harjot/vectormaster/utilities/legacyparser/PathParser.java<br>com/gatheringhallstudios/mhworlddatabase/features/workshop/selectors/WorkshopSelectorViewModel.java<br>com/gatheringhallstudios/mhworlddatabase/util/pager/GenericPagerAdapter.java<br>com/gatheringhallstudios/mhworlddatabase/util/pager/BasePagerFragment.java<br>com/gatheringhallstudios/mhworlddatabase/data/AppConverters.java<br>com/michaelflisar/changelog/internal/ParcelUtil.java<br>com/gatheringhallstudios/mhworlddatabase/features/kinsects/KinsectTreeAdapter.java<br>com/gatheringhallstudios/mhworlddatabase/features/search/UniversalSearchViewModel.java<br>com/michaelflisar/changelog/ChangelogParserUtil.java<br>butterknife/ButterKnife.java<br>com/gatheringhallstudios/mhworlddatabase/components/SkillLevelView.java<br>com/michaelflisar/changelog/ChangelogBuilder.java<br>com/gatheringhallstudios/mhworlddatabase/ass |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | OWASP MASVS: MSTG-STORAGE-3 | ets/ColoredVectorDrawable$basePath$2.java<br>com/sdsmdg/harjot/vectormaster/utilities/parser/PathParser.java<br>com/gatheringhallstudios/mhworlddatabase/util/Functions$loggedThread$1.java<br>com/gatheringhallstudios/mhworlddatabase/util/sqliteloader/sqliteasset/VersionComparator.java<br>com/gatheringhallstudios/mhworlddatabase/features/weapons/WeaponTreeAdapter.java<br>com/gatheringhallstudios/mhworlddatabase/components/HeaderItemDivider.java<br>com/gatheringhallstudios/mhworlddatabase/assets/AssetExtensionsKt.java<br>com/gatheringhallstudios/mhworlddatabase/util/Functions$createLiveData$$inlined$loggedThread$1.java<br>com/gatheringhallstudios/mhworlddatabase/util/sqliteloader/sqliteasset/Utils.java<br>com/michaelflisar/changelog/internal/ChangelogParserAsyncTask.java<br>com/gatheringhallstudios/mhworlddatabase/util/sqliteloader/sqliteasset/SQLiteAssetHelper.java |
| 2 | Files may contain hardcoded sensitive information like usernames, passwords, keys etc. | warning | CWE: CWE-312: Cleartext Storage of Sensitive Information<br>OWASP Top 10: M9: Reverse Engineering<br>OWASP MASVS: MSTG-STORAGE-14 | com/michaelflisar/changelog/internal/ChangelogPreferenceUtil.java<br>com/gatheringhallstudios/mhworlddatabase/data/entities/SkillTreeEntity.java<br>com/gatheringhallstudios/mhworlddatabase/data/dao/SkillDao.java |
| 3 | App can write to App Directory. Sensitive Information should be encrypted. | info | CWE: CWE-276: Incorrect Default Permissions<br>OWASP MASVS: MSTG-STORAGE-14 | com/gatheringhallstudios/mhworlddatabase/AppSettings.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 4 | 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')<br>OWASP Top 10: M7: Client Code Quality | com/gatheringhallstudios/mhworlddatabase/util/sqliteloader/adapters/FrameworkSQLiteDatabase.java<br>com/gatheringhallstudios/mhworlddatabase/util/sqliteloader/sqliteasset/SQLiteAssetHelper.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. |

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|
| 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. |
| 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<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**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.