MOBSF

# ANDROID STATIC ANALYSIS REPORT

## Minetest Mods (1.8.0)

| | |
|---|---|
| File Name: | installer3775.apk |
| Package Name: | com.rubenwardy.minetestmodmanager |
| Scan Date: | May 31, 2022, 7:51 p.m. |
| App Security Score: | 65/100 (LOW RISK) |
| Grade: | A |

## FINDINGS SEVERITY

| HIGH | MEDIUM | INFO | SECURE | HOTSPOT |
|---|---|---|---|---|
| 1 | 3 | 1 | 2 | 1 |

## FILE INFORMATION

**File Name:** installer3775.apk
**Size:** 2.11MB
**MD5:** ccfd223ed8bac3f69b9bca5dc735e2c6
**SHA1:** 36d6d0db018a86d3e6059983315c5469ae19e994
**SHA256:** f5583b59f5632e08bf1262eeaaaef97c267c75595077fb4476b2652c9f6933f7

## APP INFORMATION

**App Name:** Minetest Mods
**Package Name:** com.rubenwardy.minetestmodmanager
**Main Activity:** com.rubenwardy.minetestmodmanager.views.ModListActivity
**Target SDK:** 21
**Min SDK:** 14
**Max SDK:**
**Android Version Name:** 1.8.0
**Android Version Code:** 19

# APP COMPONENTS

**Activities:** 7
**Services:** 1
**Receivers:** 1
**Providers:** 0
**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: 2016-04-10 18:02:06+00:00
Valid To: 2043-08-27 18:02:06+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x24d3a353
Hash Algorithm: sha256
md5: ae9f80be16881bf8fe822ff4478e9205
sha1: 984dce98ebf98857b45d7ca456578c8fde68288f
sha256: 3af75aab93f271e10b31139745cdf599019e9637174ca7b7fb07b39253adb5f2
sha512: 1882664e174b1f9f39fe8b4434a74a425260ad9b0be6aa9d3a4656ce5e46a5e617c09669fe21d692ebd30fca3f4bdee38edc76b4b4b2d463c699218f4d3d7548

| 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. |

## APPLICATION PERMISSIONS

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| android.permission.WRITE_EXTERNAL_STORAGE | dangerous | read/modify/delete external storage contents | Allows an application to write to external storage. |
| android.permission.INTERNET | normal | full Internet access | Allows an application to create network sockets. |

## 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 |
|---|---|---|---|---|

| 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/rubenwardy/minetestmodmanager/manager/Utils.java<br>com/rubenwardy/minetestmodmanager/views/ReportActivity.java<br>com/rubenwardy/minetestmodmanager/restapi/StoreAPI.java<br>com/rubenwardy/minetestmodmanager/presenters/ModListPresenter.java<br>com/rubenwardy/minetestmodmanager/models/MinetestDepends.java<br>com/rubenwardy/minetestmodmanager/views/ModDetailFragment.java<br>com/rubenwardy/minetestmodmanager/models/MinetestConf.java<br>com/rubenwardy/minetestmodmanager/views/SettingsAndAboutActivity.java<br>com/rubenwardy/minetestmodmanager/manager/ServiceResultReceiver.java<br>com/rubenwardy/minetestmodmanager/presenters/DisclaimerPresenter.java<br>com/rubenwardy/minetestmodmanager/manager/ModManager.java<br>org/greenrobot/eventbus/EventBus.java<br>com/rubenwardy/minetestmodmanager/views/ModListActivity.java<br>com/rubenwardy/minetestmodmanager/views/ModDetailActivity.java<br>org/greenrobot/eventbus/BackgroundPoster.java<br>com/rubenwardy/minetestmodmanager/manager/ModInstallService.java<br>com/rubenwardy/minetestmodmanager/models/ModList.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 2 | App can read/write to External Storage. Any App can read data written to External Storage. | warning | CWE: CWE-276: Incorrect Default Permissions<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | com/rubenwardy/minetestmodmanager/views/WorldConfigActivity.java<br>com/rubenwardy/minetestmodmanager/presenters/ModListPresenter.java |
| 3 | This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel. | secure | OWASP MASVS: MSTG-NETWORK-4 | com/rubenwardy/minetestmodmanager/restapi/StoreAPIBuilder.java |

## NIAP ANALYSIS v1.3

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|
| 1 | FCS_STO_EXT.1.1 | Security Functional Requirements | Storage of Credentials | The application does not store any credentials to non-volatile memory. |
| 2 | FCS_CKM_EXT.1.1 | Security Functional Requirements | Cryptographic Key Generation Services | The application generate no asymmetric cryptographic keys. |
| 3 | FDP_DEC_EXT.1.1 | Security Functional Requirements | Access to Platform Resources | The application has access to ['network connectivity']. |
| 4 | FDP_DEC_EXT.1.2 | Security Functional Requirements | Access to Platform Resources | The application has access to no sensitive information repositories. |

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|
| 5 | FDP_NET_EXT.1.1 | Security Functional Requirements | Network Communications | The application has user/application initiated network communications. |
| 6 | 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. |
| 7 | 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. |
| 8 | 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. |
| 9 | FCS_COP.1.1(2) | Selection-Based Security Functional Requirements | Cryptographic Operation - Hashing | The application perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits. |
| 10 | FCS_HTTPS_EXT.1.2 | Selection-Based Security Functional Requirements | HTTPS Protocol | The application implement HTTPS using TLS. |
| 11 | FCS_HTTPS_EXT.1.3 | Selection-Based Security Functional Requirements | HTTPS Protocol | The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid. |
| 12 | FIA_X509_EXT.2.1 | Selection-Based Security Functional Requirements | X.509 Certificate Authentication | The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS. |

## 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 |
| minetest-mods.rubenwardy.com | ok | **IP:** 194.36.147.174<br>**Country:** Germany<br>**Region:** Hessen<br>**City:** Frankfurt am Main<br>**Latitude:** 50.115520<br>**Longitude:** 8.684170<br>**View:** Google Map |

## HARDCODED SECRETS

| POSSIBLE SECRETS |
|---|
| "modinfo_details_author" : "Author" |
| "modinfo_details_author" : "Autor" |
| "modinfo_details_author" : "Auteur" |
| "modinfo_details_author" : "Autor" |

## 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.