

## ANDROID STATIC ANALYSIS REPORT



Minetest Mods (1.9.1)

File Name:	installer3851.apk
Package Name:	com.rubenwardy.minetestmodmanager
Scan Date:	May 31, 2022, 7:05 p.m.
App Security Score:	65/100 (LOW RISK)
Grade:	A

#### FINDINGS SEVERITY

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

#### FILE INFORMATION

File Name: installer3851.apk

Size: 2.47MB

MD5: 0936efa4ab56aef2dc9dae0220e7d7c4

**SHA1**: b0b7c6933b092b2758b8e3dbac7515f3e8364727

SHA256: 54a8a0204bbbae9f95d999250f301f93d248b8ceeedae2aaf5b2aef3fff32b9a

### **i** APP INFORMATION

App Name: Minetest Mods

Package Name: com.rubenwardy.minetestmodmanager

 $\textbf{\textit{Main Activity}}: com.rubenwardy.minetest mod manager.views. Splash Activity$ 

Target SDK: 28 Min SDK: 14 Max SDK:

Android Version Name: 1.9.1
Android Version Code: 23

#### **EE** APP COMPONENTS

Activities: 8
Services: 1
Receivers: 1
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: 2016-04-10 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.	

## **命 APKID ANALYSIS**

FILE	DETAILS			
classes.dex	FINDINGS DETAILS			
	Compiler	r8		



NO	SCOPE	SEVERITY	DESCRIPTION	

# **Q** 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 OWASP MASVS: MSTG-STORAGE-3	com/rubenwardy/minetestmodmanager/views/Rep ortActivity.java com/rubenwardy/minetestmodmanager/restapi/Sto reAPI.java com/rubenwardy/minetestmodmanager/presenters /ModListPresenter.java com/rubenwardy/minetestmodmanager/models/Mi netestConf.java com/rubenwardy/minetestmodmanager/views/Mod DetailFragment.java com/rubenwardy/minetestmodmanager/models/Mi netestDepends.java com/rubenwardy/minetestmodmanager/manager/S erviceResultReceiver.java com/rubenwardy/minetestmodmanager/presenters /DisclaimerPresenter.java com/rubenwardy/minetestmodmanager/manager/ ModManager.java com/rubenwardy/minetestmodmanager/views/Mod ListActivity.java com/rubenwardy/minetestmodmanager/views/Mod DetailActivity.java com/rubenwardy/minetestmodmanager/views/Mod DetailActivity.java com/rubenwardy/minetestmodmanager/views/Setti ngsAndAboutActivity.java com/rubenwardy/minetestmodmanager/manager/ ModInstallService.java com/rubenwardy/minetestmodmanager/manager/ ModInstallService.java com/rubenwardy/minetestmodmanager/manager/ ModInstallService.java com/rubenwardy/minetestmodmanager/manager/ Utils.java
2	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/rubenwardy/minetestmodmanager/views/Wor ldConfigActivity.java com/rubenwardy/minetestmodmanager/presenters /ModListPresenter.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/Sto reAPIBuilder.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.
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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
10	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.
11	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.

# **Q DOMAIN MALWARE CHECK**

DOMAIN	STATUS	GEOLOCATION
hosted.weblate.org	ok	IP: 116.203.108.97 Country: Germany Region: Bayern City: Gunzenhausen Latitude: 48.323330 Longitude: 11.601220 View: Google Map

DOMAIN	STATUS	GEOLOCATION
minetest-mods.rubenwardy.com	ok	IP: 194.36.147.174 Country: Germany Region: Hessen City: Frankfurt am Main Latitude: 50.115520 Longitude: 8.684170 View: Google Map
content.minetest.net	ok	IP: 194.36.147.174 Country: Germany Region: Hessen City: Frankfurt am Main Latitude: 50.115520 Longitude: 8.684170 View: Google Map
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
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



POSSIBLE SECRETS		
"modinfo_details_author" : "Author"		
"modinfo_details_author" : "Autor"		
"modinfo_details_author" : "Autor"		
"modinfo_details_author" : "Autor"		
"modinfo_details_author" : "Auteur"		
"modinfo_details_author" : "Yazar"		
"modinfo_details_author" : "Autor"		
"modinfo_details_author" : "Pencipta"		
"modinfo_details_author" : "Autore"		

#### 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.