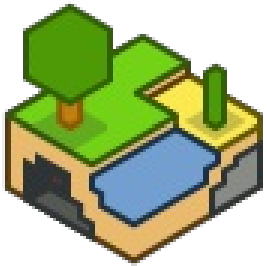
MOBSF

ANDROID STATIC ANALYSIS REPORT



Minetest (5.3.0)

File Name:	installer300.apk
Package Name:	net.minetest.minetest
Scan Date:	May 31, 2022, 10:40 a.m.
App Security Score:	44/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	2	0	1	1

FILE INFORMATION

File Name: installer300.apk
Size: 13.55MB
MD5: 788e7d6cbe56a6f9cbf69e5c187b4d96
SHA1: cf6473213c6fd8caa12c59dead14e2f0aa18f771
SHA256: 334eb70b5d66153d7ad1d580af808e1dfcd504f66600fc58187f9e38415203c3

APP INFORMATION

App Name: Minetest
Package Name: net.minetest.minetest
Main Activity: net.minetest.minetest.MainActivity
Target SDK: 29
Min SDK: 16
Max SDK:
Android Version Name: 5.3.0
Android Version Code: 31

APP COMPONENTS

Activities: 3
Services: 1
Receivers: 0
Providers: 0
Exported Activities: 1
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=FR, ST=Unknown, L=Paris, O=Minetest, OU=Minetest Core-Devs, CN=nrz
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-03-14 17:48:51+00:00
Valid To: 2040-03-07 17:48:51+00:00
Issuer: C=FR, ST=Unknown, L=Paris, O=Minetest, OU=Minetest Core-Devs, CN=nrz
Serial Number: 0x500c894b
Hash Algorithm: sha256
md5: f7acc48c74639c3a504dd9a092159d4f
sha1: 27c2aa67d2965e4e20f991201b16640e172c835a
sha256: 5323d1a1b4f68be97639eec667edf7e4e1741a8cf5223d1792da5d1f1d6e41a7
sha512: 4cca3bdd9034149348d6863e35ef1d4876b856bf79524c78d101ac9f231955ab5f302861fdf1b130aaeba06d8acba3599d33cf9b08add46dcceb5cb79a7ae632

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

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Compiler — DETAILS: r8

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Launch Mode of Activity (net.minetest.minetest.GameActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
2	Activity (net.minetest.minetest.GameActivity) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	net/minetest/minetest/UnzipService.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/arm64-v8a/libMinetest.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__FD_ISSET_chk', '__memmove_chk', '__strlen_chk', '__vsprintf_chk', '__strcat_chk', '__strchr_chk', '__memcpy_chk', '__FD_SET_chk', '__memset_chk', '__strcpy_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/arm64-v8a/libc++_shared.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk', '__read_chk']	True info Symbols are stripped.

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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.
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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
wiki.minetest.net	ok	**IP:** 51.159.52.190 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
www.collada.org	ok	**IP:** 188.114.97.0 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **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

EMAILS

EMAIL	FILE
ftp@example.com	lib/arm64-v8a/libMinetest.so

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.