

ANDROID STATIC ANALYSIS REPORT



SuperTuxKart (1.2)

File Name:	installer24.apk
Package Name:	org.supertuxkart.stk
Scan Date:	May 31, 2022, 3:06 p.m.
App Security Score:	70/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	्र HOTSPOT
0	5	2	2	2

FILE INFORMATION

File Name: installer24.apk

Size: 111.09MB

MD5: 84274bc34b7526b4bc09b1be08a248d0

SHA1: 59186ae9dc9afc14854fd589ef9462a124619fd9

SHA256: ca1e76285580947a6b25692ca0ead8fd02b2b8678c104337d5190f3f3152a57f

i APP INFORMATION

App Name: SuperTuxKart

Package Name: org.supertuxkart.stk

Main Activity: org.supertuxkart.stk.SuperTuxKartActivity

Target SDK: 29 Min SDK: 21 Max SDK:

Android Version Name: 1.2 Android Version Code: 197

B APP COMPONENTS

Activities: 1 Services: 0 Receivers: 0 Providers: 0

Exported Activities: O Exported Services: O Exported Receivers: O Exported Providers: O

***** CERTIFICATE INFORMATION

APK is signed v1 signature: True v2 signature: True v3 signature: False

Found 1 unique certificates

Subject: C=PL, ST=None, L=None, O=Deve, OU=Deve, CN=Dawid Gan

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2014-12-29 19:22:05+00:00 Valid To: 2042-05-16 19:22:05+00:00

Issuer: C=PL, ST=None, L=None, O=Deve, OU=Deve, CN=Dawid Gan

Serial Number: 0x7a2bb80 Hash Algorithm: sha256

md5: 7aff4927b2e35093f2d5d4b4d0a4928a

sha1: ed5628fefd30e42f24fda798d77cca3ca5dd4249

sha256: 326b6dc20bfee3eda6bf25624e164a2a266e3f7a094d6fded99dda29da92f8bb

sha512; b1dcdc3c53f1b17cc8fd33e7be625d7551bb797b31d4a3c8ac189ce1d01f56adc67a06b202782cf5aa00d98c0f3b11edde16bb3049655c978a5e40c4d4b6d2a2

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: a17e5827dc333d08cd1acb81e43e61b4e5c20addd2716b72dc61585a416957f4

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.

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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.
android.permission.BLUETOOTH	android.permission.BLUETOOTH normal		Allows applications to connect to paired bluetooth devices.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.



FILE	DETAILS		
	FINDINGS DETAILS		
classes.dex	Compiler	r8	

△ NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

Q MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	org/minidns/dane/ExpectingTrustManag er.java
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	org/minidns/util/CollectionsUtil.java org/minidns/AbstractDnsClient.java org/minidns/iterative/IterativeDnsClient. java
3	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	org/libsdl/app/SDLAudioManager.java org/libsdl/app/SDLActivity.java org/libsdl/app/SDLHapticHandler_API26. java org/libsdl/app/SDLMain.java org/libsdl/app/HIDDeviceBLESteamCont roller.java org/libsdl/app/SDLSurface.java org/libsdl/app/HIDDeviceUSB.java org/libsdl/app/HIDDeviceManager.java
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	org/minidns/DnsClient.java
5	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	org/minidns/AbstractDnsClient.java
6	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	org/libsdl/app/SDLClipboardHandler_AP l11.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/arm64-v8a/libmain.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', 'FD_SET_chk']	True info Symbols are stripped.

■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided 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 ['network connectivity', 'bluetooth', 'USB'].
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 user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	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.
12	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
13	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
14	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.
15	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The certificate path must terminate with a trusted CA certificate'].
16	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
supertuxkart.net	ok	IP: 185.199.110.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map



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

© 2022 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.