

ANDROID STATIC ANALYSIS REPORT



2 Player Battle (1.0.0)

File Name:	installer362.apk
Package Name:	ir.hsn6.tpb
Scan Date:	May 31, 2022, 8:04 a.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

飛 HIGH	▲ MEDIUM	i INFO	✓ SECURE	♥ HOTSPOT
2	4	2	2	0

FILE INFORMATION

File Name: installer362.apk

Size: 16.3MB

MD5: 9320d0dd6ddacef5066452de909acf87

SHA1: 0453dbca25844b2da000101a5adfe8fe3a57b4d7

SHA256: 9de8a5f0d3c9824251311883f8f480a5f83cbcdbe8b7560ab1139e92f8ccb563

i APP INFORMATION

App Name: 2 Player Battle Package Name: ir.hsn6.tpb

Main Activity: com.godot.game.GodotApp

Target SDK: 28 Min SDK: 18 Max SDK:

Android Version Name: 1.0.0 Android Version Code: 1

APP COMPONENTS

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

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: 2020-04-21 12:42:28+00:00 Valid To: 2047-09-07 12:42:28+00:00

Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Serial Number: 0x73695319 Hash Algorithm: sha256

md5: 0e5355150c7a5e02ef6ae39c4cfcaa27

sha1: aa154fdedd461ba5c6e2a52033c2312ab4b69fd7

sha256: 4c3afcf476a54276d5f49a892c0ee80a1a22687064cdc839d3250a8b8267fb88

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.

M APKID ANALYSIS

FILE	DETAILS				
classes.dex	FINDINGS	DETAILS			
classes.ucx	Compiler	r8			

△ NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

Q MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION	
----	-------	----------	-------------	--

NO	ISSUE	SEVERITY	DESCRIPTION
1	Launch Mode of Activity (com.godot.game.GodotApp) 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.

</> 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 OWASP MASVS: MSTG-STORAGE-3	org/godotengine/godot/utils/GLUtils.java org/godotengine/godot/payments/ReleaseAllCo nsumablesTask.java org/godotengine/godot/GodotDownloaderServic e.java org/godotengine/godot/payments/PaymentsMa nager.java org/godotengine/godot/xr/regular/RegularConte xtFactory.java org/godotengine/godot/GodotPaymentV3.java org/godotengine/godot/utils/GodotNetUtils.java org/godotengine/godot/xr/regular/RegularFallba ckConfigChooser.java org/godotengine/godot/payments/PurchaseTask .java org/godotengine/godot/ttils/HttpRequester.java org/godotengine/godot/GodotDownloaderAlarm Receiver.java org/godotengine/godot/GodotIO.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	org/godotengine/godot/GodotDownloaderServic e.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	org/godotengine/godot/utils/CustomSSLSocketF actory.java
4	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	org/godotengine/godot/Godot.java org/godotengine/godot/GodotlO.java
5	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	org/godotengine/godot/Godot.java
6	MD5 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/godotengine/godot/Godot.java org/godotengine/godot/utils/Crypt.java
7	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/godotengine/godot/utils/Crypt.java



NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/armeabi- v7a/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.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/armeabi- v7a/libgodot_android.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.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	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 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.
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.

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_CKM.1.1(3),FCS_CKM.1.2(3)	Selection-Based Security Functional Requirements	Password Conditioning	A password/passphrase shall perform [Password-based Key Derivation Functions] in accordance with a specified cryptographic algorithm
12	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
13	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
www.gamblify.com	ok	IP: 3.248.8.137 Country: Ireland Region: Dublin City: Dublin Latitude: 53.343990 Longitude: -6.267190 View: Google Map
godotengine.org	ok	IP: 212.85.158.4 Country: France Region: Ile-de-France City: Paris Latitude: 48.853409 Longitude: 2.348800 View: Google Map
www.moonwards.com	ok	IP: 173.236.152.49 Country: United States of America Region: California City: Brea Latitude: 33.930222 Longitude: -117.888420 View: Google Map
heroiclabs.com	ok	IP: 35.241.38.245 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map

DOMAIN	STATUS	GEOLOCATION
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
schemas.xmlsoap.org	ok	IP: 13.107.246.67 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
interblockgaming.com	ok	IP: 91.185.213.138 Country: Slovenia Region: Ljubljana City: Ljubljana Latitude: 46.051079 Longitude: 14.505130 View: Google Map

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.