ANDROID STATIC ANALYSIS REPORT

Screeps (0.0.3)

File Name:	installer3846.apk
Package Name:	eu.ryuu.screeps
Scan Date:	May 31, 2022, 7 p.m.
App Security Score:	42/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	ℹ INFO	✓ SECURE	HOTSPOT
2	1	0	1	0

FILE INFORMATION

File Name: installer3846.apk
Size: 4.58MB
MD5: b0e766231aa8c5937c5e71ef95d168f8
SHA1: 87c87bbd647a9aa95666c2569929960b2ae60dfd
SHA256: d0bbc3244c840d17ee068ac7b6b4bfe3924c0a2fe35d7dced38557cbce2132ee

APP INFORMATION

App Name: Screeps
Package Name: eu.ryuu.screeps
Main Activity: eu.ryuu.screeps.MainActivity
Target SDK: 28
Min SDK: 19
Max SDK:
Android Version Name: 0.0.3
Android Version Code: 3

APP COMPONENTS

Activities: 1
Services: 0
Receivers: 0
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: 2019-07-06 09:31:16+00:00
Valid To: 2046-11-21 09:31:16+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x5a82027f
Hash Algorithm: sha256
md5: 5a1621d3bc5de0589dbdb3e8f8ab9e55
sha1: f58f759a9ad85bc51fa028b1d85725e0f496b764
sha256: c93779634da7d0ab7a34e0dcec8a0d32de34db09da74457e6a7dd712e83b9e33
sha512: a80e19ce0eeeaa24baefe7238c406971c225b936904737985e4188ffbc2b5944cb83471bdbe423fcb5a6a4b8c265e7a1f56e572f0dbf1845ba0a7241529e328f
```

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.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th colspan="2">DETAILS</th></tr>
<tr><td rowspan="3">classes.dex</td><td>FINDINGS</td><td>DETAILS</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
2	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

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'].
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	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
9	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.
10	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.

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.