



# ANDROID STATIC ANALYSIS REPORT



 Spider (0.2.0)

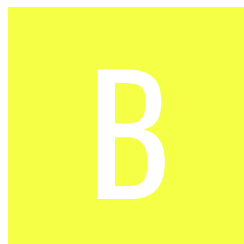
File Name: installer303.apk

Package Name: org.kknickkk.spider






Scan Date: May 31, 2022, 9:56 a.m.

App Security Score: 46/100 (MEDIUM RISK)

Grade:



## FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
2	6	1	1	1

## FILE INFORMATION

File Name: installer303.apk

Size: 2.0MB

MD5: b4ea194c8ce0ebfe91e76b7042c72dd2

SHA1: 35b539e1115e14d4bdee94326268fa668d90e04e

SHA256: 7cc5bd7f7e20b2efad5ee600b1e836443dbe15181cc84e6a36459b9e12951f34

## APP INFORMATION

App Name: Spider

Package Name: org.kknickkk.spider

Main Activity: org.kknickkk.spider.RegisterActivity

Target SDK: 29

Min SDK: 19

Max SDK:

Android Version Name: 0.2.0

Android Version Code: 11

## APP COMPONENTS

Activities: 2

Services: 0

Receivers: 0

Providers: 1

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: 2019-12-07 16:23:55+00:00

Valid To: 2047-04-24 16:23:55+00:00

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

Serial Number: 0x3b3e3919

Hash Algorithm: sha256

md5: 4e6c9621c67c8211367caf880c266b37

sha1: a0bd929dc5775739fece51a4418197d500914c4f

sha256: f219c814bb2b772faf7c364e4b34111a812739ca74011dab7cf4aa22fac349e2

sha512: 0c48397cc751046e81007040d95b15e0cf7364afd5846380bc9a487c08999783ee06be8f259fcc4c2a953f74aca499a162d254025cd8047c8367d625d35d0b42

TITLE	SEVERITY	DESCRIPTION
Signed Application	<a href="#">info</a>	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.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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

## APKID ANALYSIS

FILE	DETAILS
------	---------

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Compiler	r8

## NETWORK SECURITY

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

## 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	<a href="#">The App logs information. Sensitive information should never be logged.</a>	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/jcraft/jsch/KeyExchange.java com/jcraft/jsch/KnownHosts.java com/jcraft/jsch/jce/HMAC.java com/jcraft/jsch/jce/SHA512.java com/jcraft/jsch/jce/SHA384.java org/kknickkk/spider/FolderActivity.java org/kknickkk/spider/Tasks/ConnectTask.java org/kknickkk/spider/Tasks/DownloadTask.java com/jcraft/jsch/ChannelSftp.java com/jcraft/jsch/DHGEX.java com/jcraft/jsch/DHECN.java com/jcraft/jsch/KeyPair.java org/kknickkk/spider/Tasks/UploadTask.java org/kknickkk/spider/RegisterActivity.java com/jcraft/jsch/jce/MD5.java com/jcraft/jsch/jcraft/HMACSHA1.java com/jcraft/jsch/DHG14.java com/jcraft/jsch/jcraft/HMACMD5.java com/jcraft/jsch/jce/SHA1.java com/jcraft/jsch/DHG1.java com/jcraft/jsch/Session.java com/jcraft/jsch/jce/SHA256.java org/kknickkk/spider/Tasks/GetFilesTask.java
2	<a href="#">Files may contain hardcoded sensitive information like usernames, passwords, keys etc.</a>	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/jcraft/jsch/KeyExchange.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	<a href="#">SHA-1 is a weak hash known to have hash collisions.</a>	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/jcraft/jsch/jce/SignatureRSA.java com/jcraft/jsch/jce/PBKDF.java com/jcraft/jsch/jce/SignatureDSA.java com/jcraft/jsch/jcraft/HMACSHA1.java com/jcraft/jsch/jce/SHA1.java
4	<a href="#">Weak Encryption algorithm used</a>	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/jcraft/jsch/jce/TripleDESCBC.java com/jcraft/jsch/jce/ARCFOUR256.java com/jcraft/jsch/jce/ARCFOUR128.java com/jcraft/jsch/jce/TripleDESCTR.java com/jcraft/jsch/jce/ARCFOUR.java
5	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/jcraft/jsch/ChannelX11.java com/jcraft/jsch/jgss/GSSContextKrb5.java com/jcraft/jsch/ChannelForwardedTCP IP.java com/jcraft/jsch/PortWatcher.java com/jcraft/jsch/Session.java com/jcraft/jsch/ChannelDirectTCPIP.java
6	<a href="#">App can read/write to External Storage. Any App can read data written to External Storage.</a>	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/kknickkk/spider/Tasks/DownloadTask.java
7	<a href="#">MD5 is a weak hash known to have hash collisions.</a>	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/jcraft/jsch/jce/MD5.java com/jcraft/jsch/jcraft/HMACMD5.java



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 implement asymmetric key generation.
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 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	<a href="#">FCS_RBG_EXT.2.1</a> , <a href="#">FCS_RBG_EXT.2.2</a>	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	<a href="#">FCS_CKM.1.1(3)</a> , <a href="#">FCS_CKM.1.2(3)</a>	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	<a href="#">FCS_COP.1.1(1)</a>	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption not in accordance with <a href="#">FCS_COP.1.1(1)</a> , AES-ECB mode is being used.
13	<a href="#">FCS_COP.1.1(2)</a>	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with <a href="#">FCS_COP.1.1(2)</a> and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
14	<a href="#">FCS_COP.1.1(3)</a>	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.



EMAIL	FILE
posix-rename@openssh.com statvfs@openssh.com hardlink@openssh.com	com/jcraft/jsch/ChannelSftp.java
auth-agent-req@openssh.com	com/jcraft/jsch/RequestAgentForwarding.java
auth-agent@openssh.com	com/jcraft/jsch/ChannelAgentForwarding.java
auth-agent@openssh.com	com/jcraft/jsch/Channel.java
zlib@openssh.com	com/jcraft/jsch/OpenSSHConfig.java
keepalive@jcraft.com no-more-sessions@openssh.com auth-agent@openssh.com zlib@openssh.com	com/jcraft/jsch/Session.java
zlib@openssh.com	com/jcraft/jsch/JSch.java

---

## 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](#).