

ANDROID STATIC ANALYSIS REPORT



BlueChat (1.1)

File Name:	installer36.apk
Package Name:	com.alexkang.bluechat
Scan Date:	May 31, 2022, 4:36 p.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

兼 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
1	1	2	1	1

FILE INFORMATION

File Name: installer36.apk

Size: 0.06MB

MD5: 534cd65bd7d54da7e1f8e3253f233074

SHA1: 1558b437d06d09c35e79ccc26d122739c36faae7

SHA256: 111bbb84a6707e82c1e5f6e6873a58b8019292288840084032dc5c18d334c733

i APP INFORMATION

App Name: BlueChat

Package Name: com.alexkang.bluechat

Main Activity: com.alexkang.bluechat.MainActivity

Target SDK: 21 Min SDK: 15 Max SDK:

Android Version Name: 1.1 Android Version Code: 2

EE APP COMPONENTS

Activities: 3 Services: 0 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: 2014-11-10 07:00:09+00:00 Valid To: 2042-03-28 07:00:09+00:00

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

Serial Number: 0x6c2f0b5f Hash Algorithm: sha256

md5: 780dd61a0f0cca609cdbc0087a61cdc6

sha1: 3356dd6d5efae63ce934b1f2f9802f016dba8697

sha512: ef69203056a875eb6778c66a76f91bc8e1e985fb957ee357e9ffd11b27e6335ec1b26b0eee988d92d6b7e5027a8e637e8d64361f51d5ec3108c91bbc283341e4

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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

命 APKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS	DETAILS	
	Compiler	dx	

△ NETWORK SECURITY

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

Q 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
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	com/alexkang/bluechat/ChatManager.java com/alexkang/bluechat/HostActivity.java com/alexkang/bluechat/ClientActivity.java
2	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	com/alexkang/bluechat/MessageFeedAda pter.java

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.
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['bluetooth'].
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 no network communications.
6	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files 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 not encrypt any data in traffic or does not transmit any data between itself and another trusted IT product.

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 | <u>Ajin Abraham</u> | <u>OpenSecurity.</u>