ANDROID STATIC ANALYSIS REPORT

KouChat (1.1.1)

File Name:	installer69.apk
Package Name:	net.usikkert.kouchat.android
Scan Date:	May 31, 2022, 1:42 p.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	6	1	1	1

FILE INFORMATION

File Name: installer69.apk
Size: 2.46MB
MD5: 2070991031d253fca693dea2976cc879
SHA1: b3ca42d7e9193eaefbbca17e359b94b8a4c6e82f
SHA256: 54b8cf4938a990b03717d2e375fe4b3d242f2a534847cca2b3411c4ef88b35e2

APP INFORMATION

App Name: KouChat
Package Name: net.usikkert.kouchat.android
Main Activity: net.usikkert.kouchat.android.controller.MainChatController
Target SDK: 27
Min SDK: 16
Max SDK:
Android Version Name: 1.1.1
Android Version Code: 16

APP COMPONENTS

Activities: 5
Services: 2
Receivers: 0
Providers: 0
Exported Activities: 1
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=NO, ST=Oslo, L=Oslo, O=N/A, OU=N/A, CN=Christian Ihle
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-11-26 20:25:36+00:00
Valid To: 2039-04-13 20:25:36+00:00
Issuer: C=NO, ST=Oslo, L=Oslo, O=N/A, OU=N/A, CN=Christian Ihle
Serial Number: 0x4ed14b40
Hash Algorithm: sha1
md5: 32b16ac2090771998a3c05dd79597c00
sha1: 25ca6cb1179049eb6c5662ceb458018109613deb
sha256: ae7f0c5059e1dd5c908acd72b1ad7d9d8f946b1a6892373daaca84ed431bf058
sha512: 9a8a24ee09446a9915fd9a1ced40c8a7332d33d3ff1b8371db5d8e989d4e3b73fe5e45ea4ed1188271d55d88855f94e8ecfdc6e98a5c2cd7656b518ad1f32757
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: f66e814b8b8b0f07519c921f0c4ae85ce333b37b6f5a551af3fd87e404fd0265
```

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.
Certificate algorithm might be vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_WIFI_MULTICAST_STATE	normal	allow Wi-Fi Multicast reception	Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table></td></tr>
</table>

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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Launch Mode of Activity (net.usikkert.kouchat.android.controller.MainChatController) 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.
3	Activity (net.usikkert.kouchat.android.controller.SendFileController) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	net/usikkert/kouchat/android/filetransfer/AndroidFileUtils.java
2	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	net/usikkert/kouchat/android/settings/AndroidSettingsSaver.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	net/usikkert/kouchat/Constants.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application use no 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 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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.gnu.org	ok	**IP:** 209.51.188.116 **Country:** United States of America **Region:** Massachusetts **City:** Boston **Latitude:** 42.358429 **Longitude:** -71.059769 **View:** Google Map
www.facebook.com	ok	**IP:** 157.240.201.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.kouchat.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

✉ EMAILS

EMAIL	FILE
contact@kouchat.net	net/usikkert/kouchat/Constants.java

EMAIL	FILE
contact@kouchat.net	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"settings_nick_name_key" : "nick_name"
"settings_notification_light_key" : "notification_light"
"settings_notification_sound_key" : "notification_sound"
"settings_notification_vibration_key" : "notification_vibration"
"settings_own_color_key" : "own_color"
"settings_sys_color_key" : "sys_color"
"settings_wake_lock_key" : "wake_lock"

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.