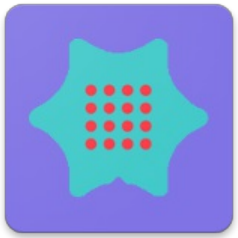
MOBSF

ANDROID STATIC ANALYSIS REPORT



Calliope mini (1.0.1)

File Name:	installer21.apk
Package Name:	cc.calliope.mini
Scan Date:	May 31, 2022, 4:01 p.m.
App Security Score:	53/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	4	1	1	1

FILE INFORMATION

File Name: installer21.apk
Size: 1.5MB
MD5: bf56e69b84dff3905b350c2caf014516
SHA1: bc205d23309ad088542476ea5edb6775ebd85bce
SHA256: b5ee1334280367b09019834b9e50a696a5eac5ca2e13d313aec9cde8ceaf3670

APP INFORMATION

App Name: Calliope mini
Package Name: cc.calliope.mini
Main Activity: cc.calliope.mini.SplashScreenActivity
Target SDK: 27
Min SDK: 18
Max SDK:
Android Version Name: 1.0.1
Android Version Code: 7

APP COMPONENTS

Activities: 9
Services: 1
Receivers: 0
Providers: 2
Exported Activities: 2
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: 2019-06-14 07:31:53+00:00
Valid To: 2046-10-30 07:31:53+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x30b65483
Hash Algorithm: sha256
md5: 0b8f3183d5a96e3e3129e1e07ea2a279
sha1: 15d2cee68b92b9bca04877287e8da7ae26bfaae5
sha256: 7a8f0b506a6138d341a956e7f3af3043ce9e82e6dbe7c949c8a72091a25bf9e3
sha512: 7fed2b5bb0a71cdc84a0011b9e18dd71cc83b527aec5dc77e37dff0d85c5b192bcf1e7092658404caf507ca248589cb69bfae846ffb7ff6bf88590fdc36d3b75

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.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
no.nordicsemi.android.LOG	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</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.
2	Activity (cc.calliope.mini.ScannerActivity) 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.
3	Activity (cc.calliope.mini.receiveFileIntentActivity) 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	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	cc/calliope/mini/selectEditorActivity.java cc/calliope/mini/ScannerActivity.java b/a/a/b/c.java b/a/a/b/b.java cc/calliope/mini/editorAcitvity.java b/a/a/a/a.java cc/calliope/mini/MBApp.java b/a/a/e/a/a/k.java cc/calliope/mini/viewmodels/SingleLiveEvent.java cc/calliope/mini/myCodeActivity.java cc/calliope/mini/profile/BlinkyManager.java cc/calliope/mini/DFUActivity.java cc/calliope/mini/viewmodels/BlinkyViewModel.java cc/calliope/mini/receiveFileIntentActivity.java cc/calliope/mini/adapter/HexFilesAdapter.java butterknife/ButterKnife.java
2	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	a/b/a/b/j.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', 'bluetooth', 'location'].
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	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
lab.open-roberta.org	ok	**IP:** 192.102.162.200 **Country:** Germany **Region:** Baden-Wurttemberg **City:** Karlsruhe **Latitude:** 49.004719 **Longitude:** 8.385830 **View:** Google Map
makecode.calliope.cc	ok	**IP:** 20.49.104.33 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map
calliope.cc	ok	**IP:** 81.169.145.79 **Country:** Germany **Region:** Berlin **City:** Berlin **Latitude:** 52.524368 **Longitude:** 13.410530 **View:** Google Map

EMAILS

EMAIL	FILE
info@calliope.cc	Android String Resource

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.