MOBSF

ANDROID STATIC ANALYSIS REPORT

BLE Peripheral Simulator (3.0)

File Name:	installer8.apk
Package Name:	io.github.webbluetoothcg.bletestperipheral
Scan Date:	May 31, 2022, 4:34 p.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	1	1	1	0

FILE INFORMATION

File Name: installer8.apk
Size: 0.06MB
MD5: dafabcc9dfbb219dfaf0347eab3ff815
SHA1: 8276581c5d98826d07b311c604e82ff17a7c59d8
SHA256: 809c20a4f5ddefb2b182d6a873a9ad4aa6aa54d0a003dbcdc8343bbb0d3c4162

APP INFORMATION

App Name: BLE Peripheral Simulator
Package Name: io.github.webbluetoothcg.bletestperipheral
Main Activity: io.github.webbluetoothcg.bletestperipheral.Peripherals
Target SDK: 22
Min SDK: 21
Max SDK:
Android Version Name: 3.0
Android Version Code: 3

APP COMPONENTS

Activities: 2
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=94043, ST=CA, L=Mountain View, O=Google, OU=Chrome, CN=Giovanni Ortuño Urquidi
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-05-26 22:35:05+00:00
Valid To: 2040-05-19 22:35:05+00:00
Issuer: C=94043, ST=CA, L=Mountain View, O=Google, OU=Chrome, CN=Giovanni Ortuño Urquidi
Serial Number: 0x390fe4da
Hash Algorithm: sha256
md5: f7f5c37a4906f98609bc6b4a0b7cb8a0
sha1: 5489779740e398ec750fdb5f1d19f9f07863a0a4
sha256: 7066ca34cb75f5c8506764f367a35265c36d5e46a72abaafe51757e4f054a8d2
sha512: 56e1400dd7620a691899722795948d9f96ab1e915d02f127fea47ddbd5902d8fda7e8c48d20ff249c56d374eccab2c02f4c428d3b0907a45fb091f5c3c69162a

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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Compiler — DETAILS: dx

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
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	io/github/webbluetoothcg/bletestperipheral/HeartRateServiceFragment.java io/github/webbluetoothcg/bletestperipheral/Peripheral.java

NIAP ANALYSIS v1.3

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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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	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 | Ajin Abraham | OpenSecurity.