MOBSF

ANDROID STATIC ANALYSIS REPORT

USB HID Terminal (1.1.1)

File Name:	installer11.apk
Package Name:	com.appspot.usbhidterminal
Scan Date:	May 30, 2022, 4:14 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	5	1	1	0

FILE INFORMATION

File Name: installer11.apk
Size: 0.81MB
MD5: 58ee67e8e4b90634d8ac7e418758336a
SHA1: 7b16e05ef77f04db2add8158fbe597617ed427b1
SHA256: a63a182a2953620c1e2c7d7f50a63f98ac2df691a199d786a9d639aa47c4c6dd

APP INFORMATION

App Name: USB HID Terminal
Package Name: com.appspot.usbhidterminal
Main Activity: com.appspot.usbhidterminal.USBHIDTerminal
Target SDK: 22
Min SDK: 12
Max SDK:
Android Version Name: 1.1.1
Android Version Code: 12

APP COMPONENTS

Activities: 2
Services: 3
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=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-08-14 06:58:33+00:00
Valid To: 2042-12-30 06:58:33+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x5bf9b21f
Hash Algorithm: sha256
md5: 69deb126c2ba09c031120fc2de242b71
sha1: e31b478769b1ac8e36c9b8d029c453e54dc3baf6
sha256: c3d61dc22f6952827a210eae9a13b81c63657f811e7bb4d52b9fdba11a47e662
sha512: 0341ae0a75bc30664b70158471c87b78896f705963dd97c294e2901c877dd417079f9ab75170f572f547c48d1e840bdd91d1a8987988cb1a9d7645cf07fab434

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.USB_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx (possible dexmerge)</td></tr><tr><td>Manipulator Found</td><td>dexmerge</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.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

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/appspot/usbhidterminal/core/services/WebServerService.java org/mockito/asm/util/ASMifierClassVisitor.java com/appspot/usbhidterminal/core/services/SocketService.java fi/iki/elonen/samples/echo/DebugWebSocket.java org/mockito/cglib/reflect/FastMethod.java com/appspot/usbhidterminal/core/webserver/WebServer.java org/mockito/asm/util/CheckClassAdapter.java org/mockito/internal/debugging/MockitoDebuggerImpl.java de/greenrobot/event/util/AsyncExecutor.java de/greenrobot/event/BackgroundPoster.java org/mockito/asm/util/TraceClassVisitor.java de/greenrobot/event/util/ErrorDialogManager.java org/mockito/internal/util/ConsoleMockitoLogger.java com/appspot/usbhidterminal/core/webserver/Ws.java fi/iki/elonen/samples/echo/EchoSocketSample.java de/greenrobot/event/util/ExceptionToResourceMapping.java com/appspot/usbhidterminal/core/services/AbstractUSBHIDService.java de/greenrobot/event/SubscriberMethodFinder.java org/mockito/cglib/core/DebuggingClassWriter.java de/greenrobot/event/EventBus.java de/greenrobot/event/util/ErrorDialogConfig.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	fi/iki/elonen/NanoHTTPD.java
3	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	fi/iki/elonen/NanoHTTPD.java org/mockito/cglib/transform/AbstractTransformTask.java
4	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	fi/iki/elonen/WebSocketResponseHandler.java
5	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	fi/iki/elonen/WebSocketResponseHandler.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.
2	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['USB', 'network connectivity'].
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 user/application initiated 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.
9	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits.

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.