MOBSF

ANDROID STATIC ANALYSIS REPORT

Mp3 Cutter (1.0)

File Name:	angel.easymp3cutter.apk
Package Name:	angel.easymp3cutter
Scan Date:	April 21, 2022, 6:04 a.m.
App Security Score:	37/100 (HIGH RISK)
Grade:	C
Trackers Detection:	1/427

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	3	0	0	1

FILE INFORMATION

File Name: angel.easymp3cutter.apk
Size: 1.22MB
MD5: 460145c5820fc360c9ae30188a3c955f
SHA1: 7ee6fe75ffb43f0225589f3529ac425c3226623d
SHA256: d302c0086ed8b5c59a5631e526a30a1957f571031a502987fa5353913bf13bc8

APP INFORMATION

App Name: Mp3 Cutter
Package Name: angel.easymp3cutter
Main Activity: .RingdroidSelectActivity
Target SDK: 21
Min SDK: 9
Max SDK:
Android Version Name: 1.0

Android Version Code: 1

APP COMPONENTS

Activities: 6
Services: 0
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: False
v3 signature: False
Found 1 unique certificates
Subject: CN=cutter
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-10-28 06:29:46+00:00
Valid To: 2099-10-07 06:29:46+00:00
Issuer: CN=cutter
Serial Number: 0x48654b50
Hash Algorithm: sha256
md5: 5a2f48cd3de096e03a328935f989d12b
sha1: fb47c67660b93acb142e5ea701e7a5e18a1ec624
sha256: b4170bbbd2dc01ed9ca66c0613b9b84cad3c28e4640e34b138af310681b48e62
sha512: d037a3ac7a2592c6009d59f21491c82681cbdbb48e220c8bde2944a176a4795677b3022d3a0c99bdcdceb77c6f248da4098bfec4efd13563fb53c3af8919ee2a

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
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.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.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
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.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check possible Build.SERIAL check</td></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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Activity (.RingdroidEditActivity) 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

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312

© 2022 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.