
Android Analysis Report



Demo app
com.termux

Date 2018-06-14

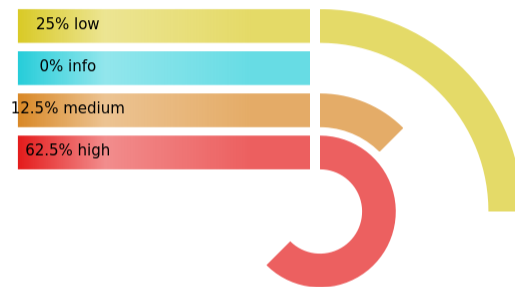
Contents

1	PERMISSIONS	1
2	FINDINGS SUMMARY	1
3	DETAILED FINDINGS	3
3.1	A1:	3
3.2	A2: Application Data can be Backed up	3
3.3	A3: Launch Mode of Activity (com. termux. app. TermuxActivity) is not standard.	4
3.4	A4: Activity (com. termux. HomeActivity) is not Protected. An intent-filter exists.	4
3.5	A5: TaskAffinity is set for Activity (com. termux. filepicker. TermuxFileReceiverActivity)	4
3.6	A6: Activity (com. termux. filepicker. TermuxFileReceiverActivity) is not Protected. An intent-filter exists.	4
3.7	A7: Content Provider (com. termux. app. TermuxOpenReceiver\$ ContentProvider) is not Protected. [android:exported=true]	5
3.8	A8:	5
4	VISUALIZATIONS	6
4.1	Chord Diagram - Class Relations	6
4.2	Hot Spot - System Overview	7

1 PERMISSIONS

Type	List
Dangerous	WRITE_EXTERNAL_STORAGE
Overprivileged	INTERNET WAKE_LOCK VIBRATE
Automatically granted dangerous permissions	READ_EXTERNAL_STORAGE

2 FINDINGS SUMMARY



Index	Title	Impact
A1		Low
A2	Application Data can be Backed up	Medium

A3	Launch Mode of Activity (com. termux. app. TermuxActivity) is not standard.	High
A4	Activity (com. termux. HomeActivity) is not Protected. An intent-filter exists.	High
A5	TaskAffinity is set for Activity (com. termux. filepicker. TermuxFileReceiverActivity)	High
A6	Activity (com. termux. filepicker. TermuxFileReceiverActivity) is not Protected. An intent-filter exists.	High
A7	Content Provider (com. termux. app. TermuxOpenReceiver\$ ContentProvider) is not Protected. [android:exported=true]	High
A8		Low

3 DETAILED FINDINGS

3.1 A1:

Description

Evidence

```
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/
smali/android/support/v4/b/a/a.smaliLandroid/util/Log->i(Ljava/lang/String;Ljava/lang/
String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/
smali/android/support/v4/b/a/a.smaliLandroid/util/Log->i(Ljava/lang/String;Ljava/lang/
String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/
smali/android/support/v4/widget/a.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/
lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/
smali/android/support/v4/view/ViewPager.smaliLandroid/util/Log->e(Ljava/lang/String;
Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/
smali/android/support/v4/view/ViewPager.smaliLandroid/util/Log->w(Ljava/lang/String;
Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/
smali/com/termux/terminal/i.smaliLandroid/util/Log->wtf(Ljava/lang/String;Ljava/lang/
String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/
smali/com/termux/terminal/i.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/
String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/
smali/com/termux/terminal/f.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/lang/
String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/
smali/com/termux/terminal/f.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/
String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/
smali/com/termux/terminal/f.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/lang/
String;)
```

snip

For the full list view `/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/report`

Recommendation

3.2 A2: Application Data can be Backed up

Description

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.

Recommendation

`android:allowBackup = False`

3.3 A3: Launch Mode of Activity (com. termux. app. TermuxActivity) is not standard.

Description

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.

Recommendation

It is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

3.4 A4: Activity (com. termux. HomeActivity) is not Protected. An intent-filter exists.

Description

A 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.

Recommendation

It is recommended to set the protection level to signature, so only applications signed with the same certificate can obtain the permission.

3.5 A5: TaskAffinity is set for Activity (com. termux. filepicker. TermuxFileReceiverActivity)

Description

If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task.

Recommendation

Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.

3.6 A6: Activity (com. termux. filepicker. TermuxFileReceiverActivity) is not Protected. An intent-filter exists.

Description

A 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.

Recommendation

It is recommended to set the protection level to signature, so only applications signed with the same certificate can obtain the permission.

3.7 A7: Content Provider (com. termux. app. TermuxOpenReceiver\$ContentProvider) is not Protected. [android:exported=true]

Description

A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

Recommendation

It is recommended to set the protection level to signature, so only applications signed with the same certificate can obtain the permission.

3.8 A8:

Description

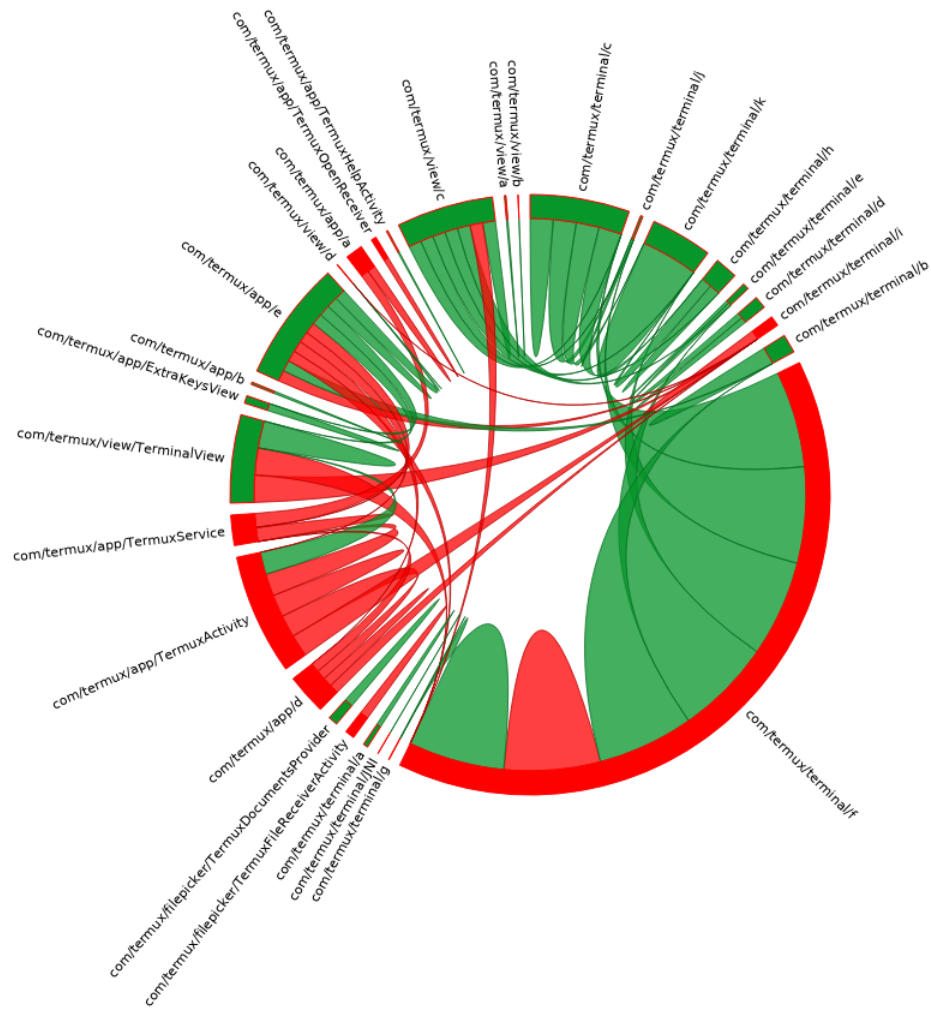
Evidence

/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/smali/android/support/v4/b/a/a.smaliinvoke

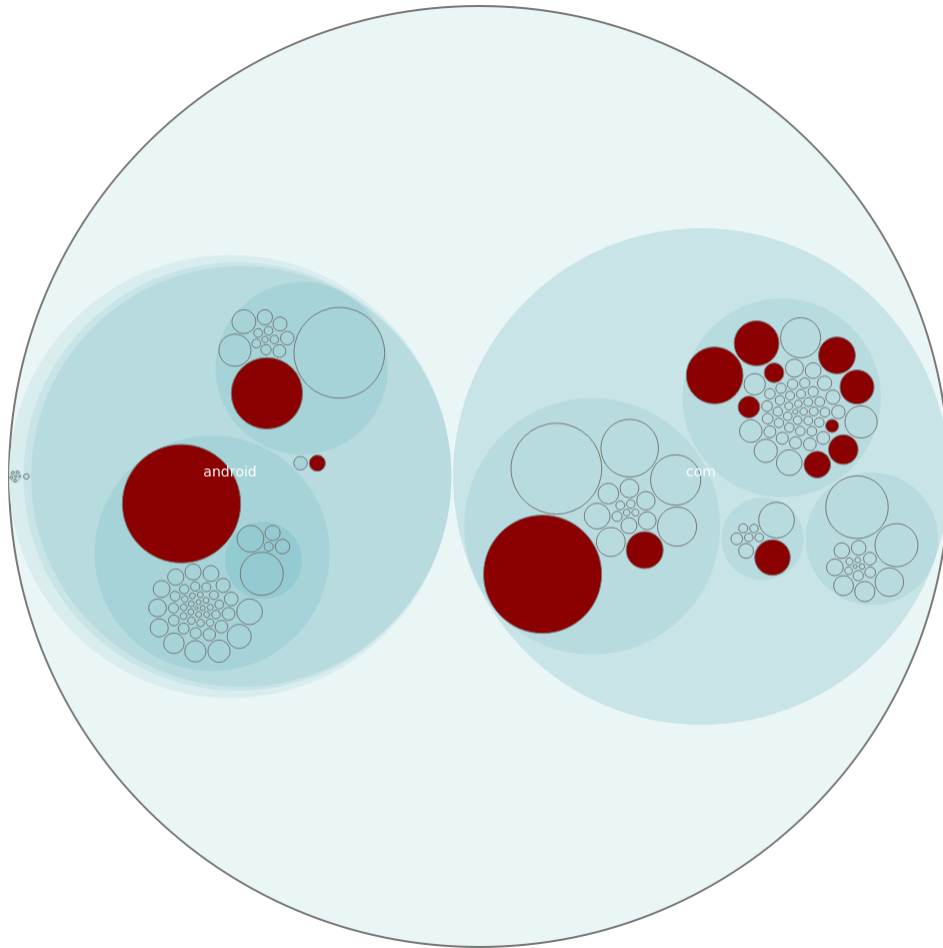
Recommendation

4 VISUALIZATIONS

4.1 Chord Diagram - Class Relations



4.2 Hot Spot - System Overview



Index	Class
1	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/smali/com/termux/terminal/f.smali
2	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/smali/com/termux/app/a\$1.smali
3	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/smali/com/termux/app/TermuxOpenReceiver.smali
4	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/smali/android/support/v4/b/a/a.smali
5	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/smali/com/termux/app/d.smali
6	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/smali/com/termux/app/c\$3.smali

```
7      /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
      apps/com_termux/app/smali/android/support/v4/view/ViewPager.smali
8      /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
      apps/com_termux/app/smali/com/termux/terminal/i.smali
9      /home/miki/Documents/GITHUB/AndroidPermissions/apks/
      playstore_apps/com_termux/app/smali/com/termux/filepicker/
      TermuxFileReceiverActivity.smali
10     /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_
      apps/com_termux/app/smali/android/support/v4/widget/a.smali
```