Android Analysis Report

AndroART

Insecure Bank

com.insecurebnk

Date 2018-06-13

Contents

1 FINDINGS SUMMARY

Index	Title	Impact
A1	Non-random XOR	**High**
A2	Radare check: emulator	**Info**
A3	Radare check: url	**Info**
A4	Radare check: root	**Info**
A5	Radare check: apk	**Info**
A6	Radare check: network	**Info**
A7	Radare check: libs	**Info**
A8	Radare check: file	**Info**
A9	Radare check: other	**Info**
A10	Radare check: api	**Info**
A11	Radare check: sms	**Info**
A12	Radare check: location	**Info**
A13	testing	**Low**
A14	Application Data can be Backed up	**Medium**
A15	Launch Mode of Activity (com.termux.app.TermuxActivity) is not standard.	**High**

A16	Activity (com. termux. HomeActivity) is not Protected. An intent-filter exists.	**High**
A17	TaskAffinity is set for Activity (com. termux. filepicker. TermuxFileReceiverActivity)	**High**
A18	Activity (com. termux. filepicker. TermuxFileReceiverActivity) is not Protected. An intent-filter exists.	**High**
A19	Content Provider (com. termux. app. TermuxOpenReceiver$ContentProvider) is not Protected. [android:exported=true]	**High**
A20		**Low**

2 DETAILED FINDINGS

2.1 A1: Non-random XOR

Description

Test description

Evidence

```
/app/smali/com/termux/view/TerminalView.smalixor-int/lit8v0,v0,-0x1
/app/smali/android/support/v4/widget/a.smalixor-int/lit8v1,v1,-0x1
/app/smali/com/termux/terminal/c.smalixor-int/lit8v3,v3,-0x1
```

Recommendation

Test recommendation

2.2 A2: Radare check: emulator

Description

Evidence

Recommendation

2.3 A3: Radare check: url

Description

Evidence

```
  0x30b0d6564?http://play.google.com/store/apps/details?id=com.termux.styling0x30b4e4140'
https://termux.net/bootstrap/bootstrap-
  0x30b782423https://wiki.termux.com
  0x30b904039&https://wiki.termux.com/wiki/Main_Page
```

Recommendation

2.4 A4: Radare check: root

Description

Evidence

Recommendation

2.5 A5: Radare check: apk

Description

Evidence

```
  0x087dex\n035
  0x2a3201211\natindex
  0x2b72e4544+Landroid/content/ActivityNotFoundException;
  0x2ba1c51501Landroid/content/res/Resources$NotFoundException;
  0x2e2763231Ljava/io/FileNotFoundException;
  0x2e4433938%Ljava/lang/IndexOutOfBoundsException;
  0x2e47f3433Ljava/lang/InterruptedException;
  0x2e4c53433Ljava/lang/NoSuchFieldException;
  0x2e4e73534!Ljava/lang/NoSuchMethodException;
  0x2ff5b1716findPointerIndex
```

snip

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

Recommendation

2.6 A6: Radare check: network

Description

Evidence

```
  0x2d2683130Landroid/webkit/WebViewClient;
  0x3020c1514getClientWidth
  0x321f61716setWebViewClient0x2b97b3736#Landroid/content/ServiceConnection;
  0x2d15f4847.Landroid/view/inputmethod/BaseInputConnection;
  0x2d1b64443*Landroid/view/inputmethod/InputConnection;
  0x311bb2423onCreateInputConnection
  0x314d31918onServiceConnected
  0x314e72221onServiceDisconnected0x2a76156556/data/data/com.termux/files/home/bin/
termux-url-opener
  0x2e7731514Ljava/net/URL;
  0x2eeff164163Thefollowingfiledoesnotexist:\n$HOME/bin/termux-url-opener\n\nCreatethisfileasasc
```

snip

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

Recommendation

2.7 A7: Radare check: libs

Description

Evidence

```
  0x30f611312\vloadLibrary
```

Recommendation

2.8 A8: Radare check: file

Description

Evidence

```
0x2ad791918Cannotopenfile:
0x2b0232120Errorsavingfile:\n\n
0x324483736#termux-open:Notareadablefile:'0x2a5fb2928\e/data/data/com.termux/files
0x2a6183433/data/data/com.termux/files/home
0x2a63a6766A/data/data/com.termux/files/home/.config/termux/termux.properties
0x2a67d6059:/data/data/com.termux/files/home/.termux/colors.properties
0x2a6b951501/data/data/com.termux/files/home/.termux/font.ttf
0x2a6ec6059:/data/data/com.termux/files/home/.termux/termux.properties
0x2a72857567/data/data/com.termux/files/home/bin/termux-file-editor
0x2a76156556/data/data/com.termux/files/home/bin/termux-url-opener
```

snip

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

Recommendation

2.9 A9: Radare check: other

Description

Evidence

```
0x2a99b1413\f;password:
0x30dd51211\nisPassword0x2a99b1413\f;password:
0x30dd51211\nisPassword
```

Recommendation

2.10 A10: Radare check: api

Description

Evidence

Recommendation

2.11 A11: Radare check: sms

Description

Evidence

Recommendation

2.12 A12: Radare check: location

Description

Evidence

Recommendation

2.13 A13: testing

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

2.14 A14: 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

2.15 A15: 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.

2.16 A16: 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.

2.17 A17: 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.

2.18 A18: 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.

2.19 A19: 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.

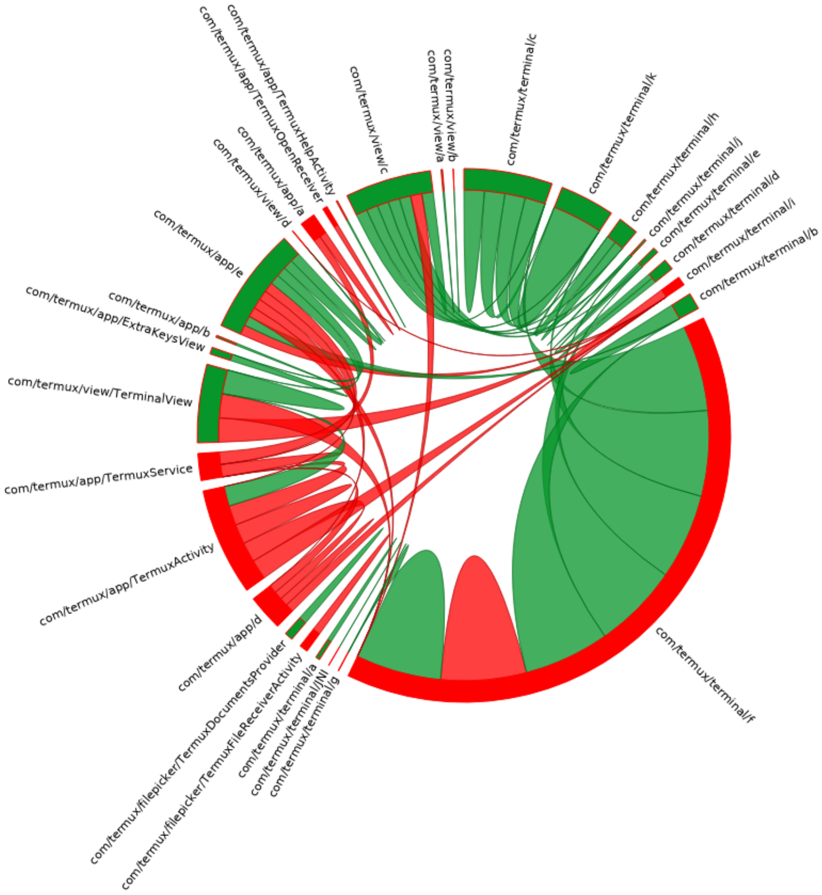
2.20 A20:

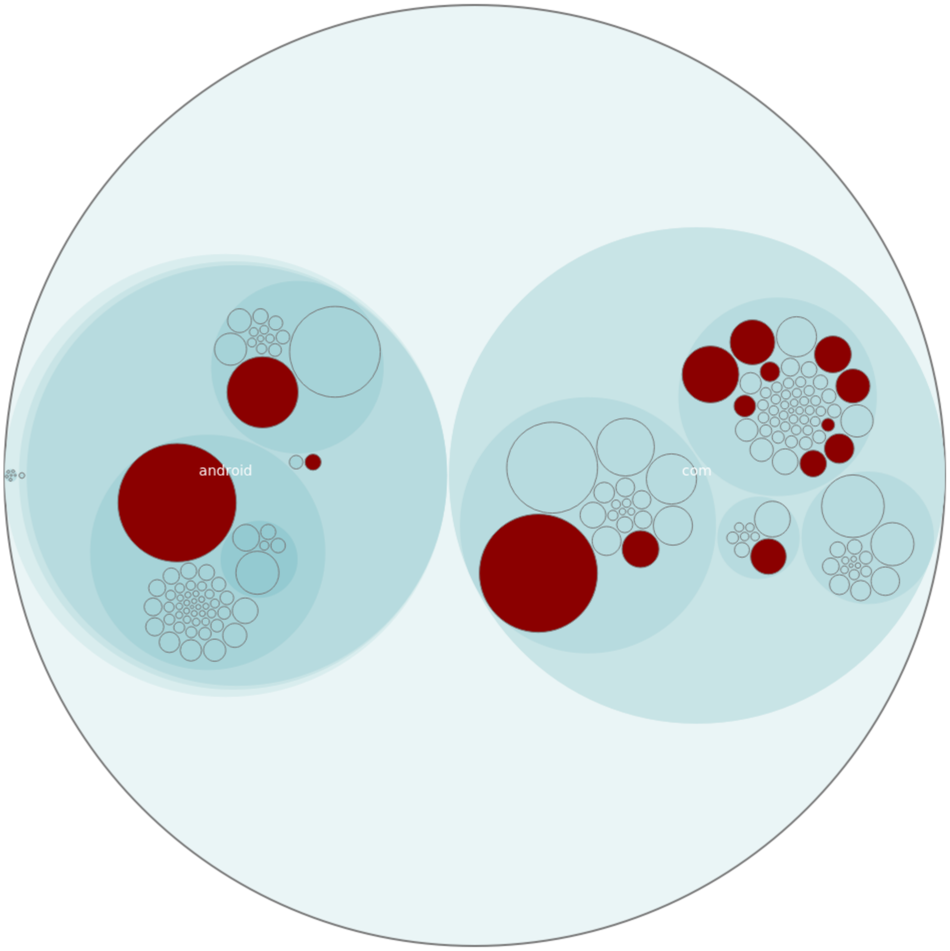
Description

Evidence

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

Recommendation





Index	Class
1	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/smali/com/termux/app/TermuxActivity$1.smali
2	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/smali/com/termux/app/TermuxActivity$1.smali
3	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/smali/com/termux/app/TermuxActivity$1.smali
4	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/smali/com/termux/app/TermuxActivity$1.smali
5	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/smali/com/termux/app/TermuxActivity$1.smali

6	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/smali/com/termux/app/TermuxActivity$1.smali
7	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/com_termux/app/smali/com/termux/app/TermuxActivity$1.smali