Android Analysis Report

Demo app

com.termux

Date 2018-06-23

Contents

1 Signature

Owner	CN=mobilepearls.com,OU=Unknown,O=MobilePearls,L=Unknown,ST=Unknown,C=SE
Issuer	CN=mobilepearls.com,OU=Unknown,O=MobilePearls,L=Unknown,ST=Unknown,C=SE
Serial Number	4bc5e4fd
MD5	26:27:7C:2D:20:44:9D:35:4F:7D:70:1A:6E:06:1C:77
SHA1	A9:66:C9:F8:87:F0:E7:EA:85:91:21:68:6F:75:2F:31:D0:69:74:0D
SHA256	73:8F:0A:30:A0:4D:3C:8A:1B:E3:04:AF:18:D0:77:9B:CF:3E:A8:8F:B6:08:08:F6:57:A3:52:18:61:C2:EB:F9
Algorithm	SHA1withRSA

2 PERMISSIONS

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

3 FINDINGS SUMMARY

Index	Title	Impact
A1	Application is using Logs	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. app. TermuxActivity) is not Protected. An intent-filter exists.	High
A5	Activity (com. termux. HomeActivity) is not Protected. An intent-filter exists.	High

A6	TaskAffinity is set for Activity (com. termux. filepicker. TermuxFileReceiverActivity)	**High**
A7	Activity (com. termux. filepicker. TermuxFileReceiverActivity) is not Protected. An intent-filter exists.	**High**
A8	Content Provider (com. termux. filepicker. TermuxDocumentsProvider) is protected by a custom permission.	**Medium**
A9	Content Provider (com. termux. app. TermuxOpenReceiver$ ContentProvider) is not Protected. [android:exported=true]	**High**
A10	Use of Reflection	**Low**

4 DETAILED FINDINGS

4.1 A1: Application is using Logs

Description

Logs were found during the analysis process. When improperly used, they may expose sensitive information such as passwords, usernames, etc.

Evidence

/home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/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/demo/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/demo/app/smali/android/support/v4/widget/a.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/app/smali/android/support/v4/view/ViewPager.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/app/smali/android/support/v4/view/ViewPager.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/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/demo/app/smali/com/termux/terminal/i.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/app/smali/com/termux/terminal/f.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/app/smali/com/termux/terminal/f.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/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/demo/report*

Recommendation

4.2 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

4.3 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.

4.4 A4: Activity (com. termux. app. TermuxActivity) 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.

4.5 A5: 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.

4.6 A6: 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.

4.7 A7: 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.

4.8 A8: Content Provider (com. termux. filepicker. TermuxDocumentsProvider) is protected by a custom permission.

Description

A Content Provider is found to be protected by a custom defined permission. The permission can be obtained by malicious apps installed prior to this one. More info at `https://github.com/commonsguy/cwac-security/blob/master/PERMS.md`

Recommendation

Failing to protect components could leave them vulnerable to attack by malicious apps.The component should be reviewed for vulnerabilities, such as injection and information leakage.

4.9 A9: 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.

4.10 A10: Use of Reflection

Description

If an attacker can supply values that the application then uses to determine which class to instantiate or which method to invoke, the potential exists for the attacker to create control flow paths through the application that were not intended by the application developers. This attack vector may allow the attacker to bypass authentication or access control checks or otherwise cause the application to behave in an unexpected manner.

Evidence

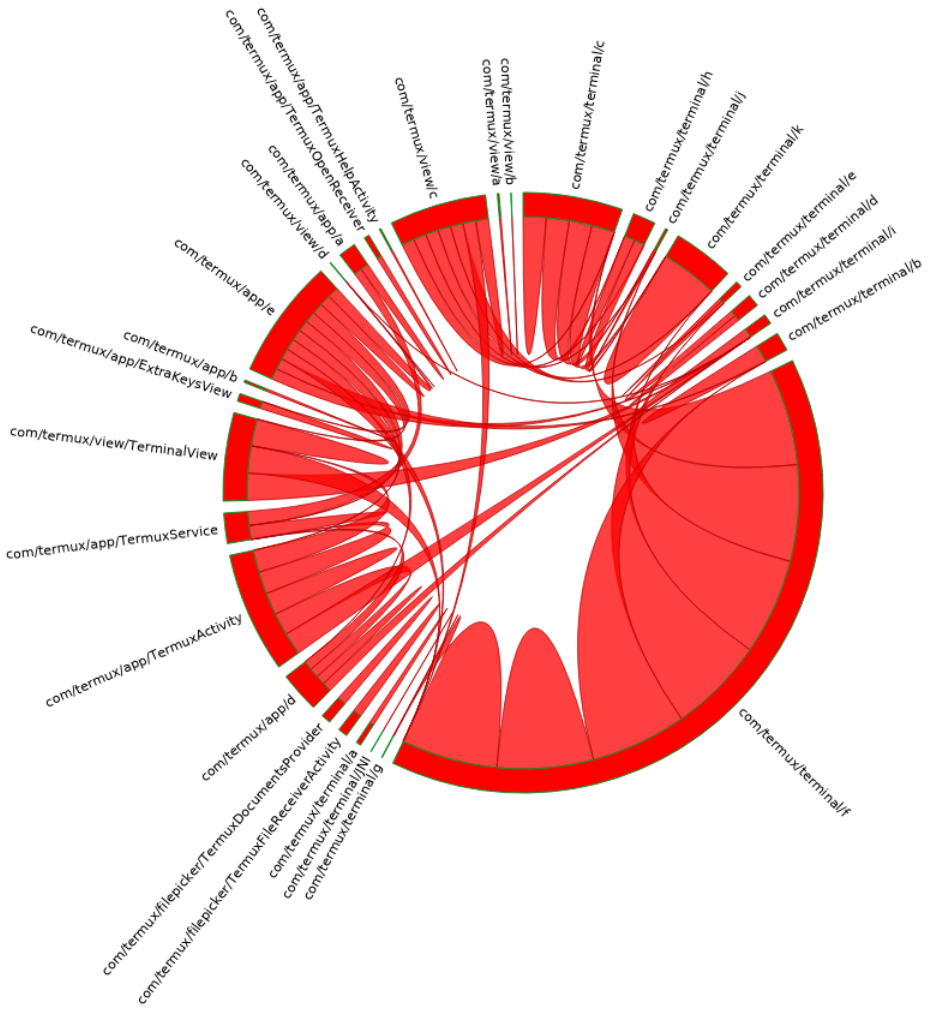
/home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/app/smali/android/support/v4/b/a/a.smaliinvoke

Recommendation

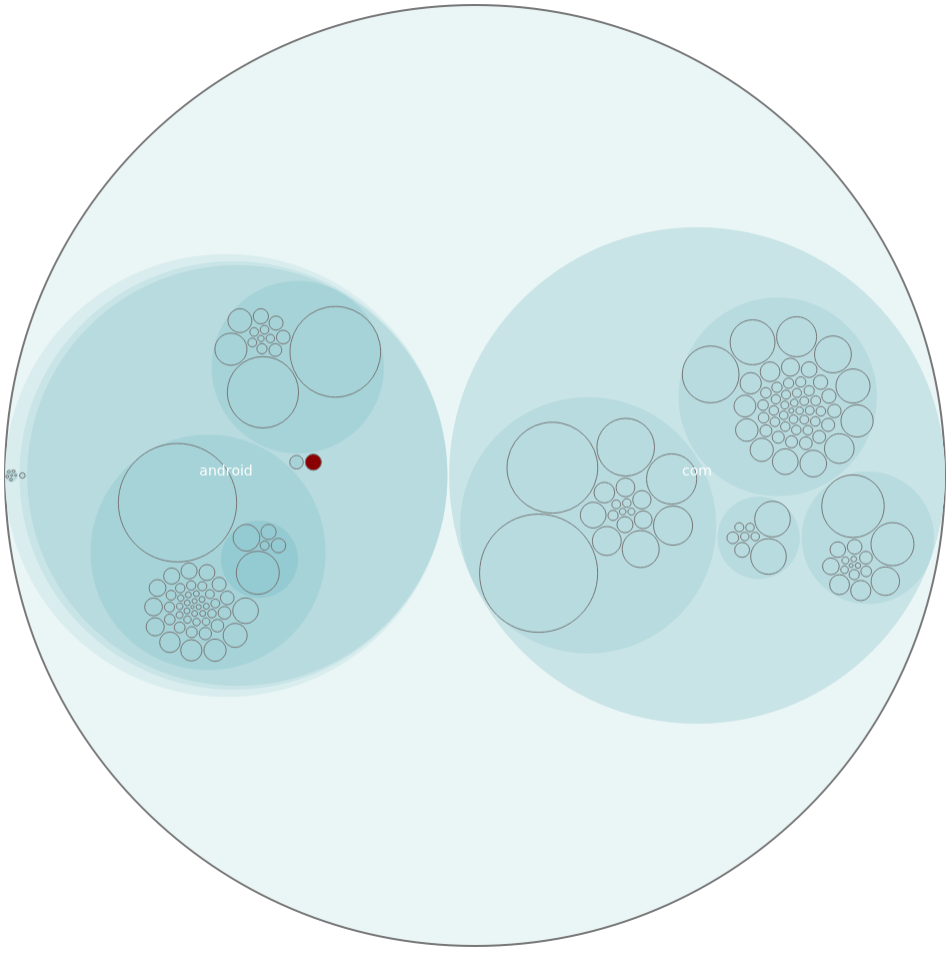
We recommend to review the usage of reflection in the application.

5 VISUALIZATIONS

5.1 Chord Diagram - Class Relations



5.2 Hot Spot - System Overview



Index	Class
1	/home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/app/smali/android/support/v4/b/a/a.smali
2	/home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/app/smali/android/a/a/c.smali
3	/home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/app/smali/android/a/a/e.smali
4	/home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/app/smali/android/a/a/b.smali
5	/home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/app/smali/android/a/a/d.smali
6	/home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/app/smali/android/a/a/a.smali

```
7   /home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/app/
    smali/android/a/a/f.smali
8   /home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/app/
    smali/android/support/v4/a/a.smali
9   /home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/app/
    smali/android/support/v4/widget/DrawerLayout$e$1.smali
10  /home/miki/Documents/GITHUB/AndroidPermissions/apks/demo/app/
    smali/android/support/v4/widget/a$1.smali
```