Android Analysis Report

Demo app

de.number26.android

Date 2018-06-14

Contents

1 Signature

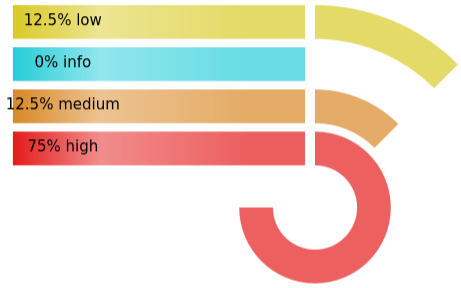
Owner	CN=JavierCuestaGomez,OU=Number26,O=Number26,L=Berlin,ST=Berlin,C=BE
Issuer	CN=JavierCuestaGomez,OU=Number26,O=Number26,L=Berlin,ST=Berlin,C=BE
Serial Number	66a19d3f
MD5	77:2D:74:B0:A9:1F:B1:2E:71:A4:57:F9:F1:F3:C7:AC
SHA1	57:6D:B8:85:4F:A2:07:97:17:6D:39:55:32:A6:1C:75:9B:DC:01:D0
SHA256	80:0F:89:B0:10:F9:EF:7C:B4:88:4E:D6:ED:CF:D0:BA:E5:0E:7F:48:4E:C0:75:17:FD:F6:61:D6:9D:65:0A:DD
Algorithm	SHA256withRSA

2 PERMISSIONS

Type	List
Normal	ACCESS_NETWORK_STATE
	ACCESS_WIFI_STATE
	INTERNET
	WAKE_LOCK
Dangerous	CAMERA
	ACCESS_COARSE_LOCATION
	ACCESS_FINE_LOCATION
	RECORD_AUDIO
	READ_EXTERNAL_STORAGE
	WRITE_EXTERNAL_STORAGE
Overprivileged	USE_FINGERPRINT
	C
	READ_CONTACTS
	BIND_GET_INSTALL_REFERRER_SERVICE
	READ_GSERVICES
	BLUETOOTH
	MODIFY_AUDIO_SETTINGS
	BLUETOOTH_ADMIN
	RECEIVE
	FLASHLIGHT
	BROADCAST_STICKY

	PUSH_MESSAGE
Underprivileged	UPDATE_DEVICE_STATS
Automatically granted dangerous permissions	WRITE_CONTACTS
	GET_ACCOUNTS

3 FINDINGS SUMMARY



Index	Title	Impact
A1	Access local ressources	**High**
A2		**Low**
A3	Launch Mode of Activity (de. number26. machete. android. ui. landing. SplashActivity) is not standard.	**High**

A4	Activity (de. number26. machete. android. deeplink. DeepLinkActivity) is not Protected. An intent-filter exists.	**High**
A5	Activity (de. number26. machete. android. ui. HomeActivity) is not Protected. An intent-filter exists.	**High**
A6	Broadcast Receiver (com. adjust. sdk. AdjustReferrerReceiver) is not Protected. [android:exported=true]	**High**
A7	Service (de. number26. machete. android. refactor. data. remote_ message. reception. FirebaseMessageCapturerService) is not Protected. An intent-filter exists.	**High**
A8	Service (de. number26. machete. android. refactor. data. remote_ message. registration. FirebaseDeviceTokenService) is not Protected. An intent-filter exists.	**High**
A9	Launch Mode of Activity (com. salesforce. android. chat. ui. internal. chatfeed. ChatFeedActivity) is not standard.	**High**
A10	Launch Mode of Activity (com. salesforce. android. chat. ui. internal. prechat. PreChatActivity) is not standard.	**High**
A11	Service (com. google. firebase. messaging. FirebaseMessagingService) is not Protected. [android:exported=true]	**High**
A12	Service (com. google. firebase. iid. FirebaseInstanceIdService) is not Protected. [android:exported=true]	**High**

A13	Activity (de. idnow. sdk. Activities_ VideoLiveStreamActivity_ IceLink) is not Protected. [android:exported=true]	**High**
A14	High Intent Priority (900) [android:priority]	**Medium**
A15	High Intent Priority (900) [android:priority]	**Medium**
A16		**Low**

4 DETAILED FINDINGS

4.1 A1: Access local ressources

Description

Evidence

/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/de/idnow/sdk/Activities_VideoLiveStreamActivity_Super.smali

Recommendation

4.2 A2:

Description

Evidence

/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/arch/lifecycle/da1.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/arch/lifecycle/da2.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/arch/lifecycle/i.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/support/v4/a/e.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/support/v4/a/e.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/support/v4/a/b$b.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/support/v4/a/b$b.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/support/v4/a/h.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/lang/String;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/support/v4/a/f.smaliLandroid/util/Log->e(Ljava/lang/String;Ljava/lang/String;Ljava/lang/Throwable;)
/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/support/v4/a/f.smaliLandroid/util/Log->w(Ljava/lang/String;Ljava/lang/String;)
snip
For the full list view /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/report

Recommendation

4.3 A3: Launch Mode of Activity (de. number26. machete. android. ui. landing. SplashActivity) 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 (de. number26. machete. android. deeplink. DeepLinkActivity) 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 (de. number26. machete. android. ui. 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: Broadcast Receiver (com. adjust. sdk. AdjustReferrerReceiver) is not Protected. [android:exported=true]

Description

A Broadcast Receiver 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.

4.7 A7: Service (de. number26. machete. android. refactor. data. remote_ message. reception. FirebaseMessageCapturerService) is not Protected. An intent-filter exists.

Description

A Service 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 Service 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: Service (de. number26. machete. android. refactor. data. remote_ message. registration. FirebaseDeviceTokenService) is not Protected. An intent-filter exists.

Description

A Service 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 Service 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.

4.9 A9: Launch Mode of Activity (com. salesforce. android. chat. ui. internal. chatfeed. ChatFeedActivity) 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.

4.10 A10: Launch Mode of Activity (com. salesforce. android. chat. ui. internal. prechat. PreChatActivity) 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.

4.11 A11: Service (com. google. firebase. messaging. FirebaseMessagingService) is not Protected. [android:exported=true]

Description

A Service 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.

4.12 A12: Service (com. google. firebase. iid. FirebaseInstanceIdService) is not Protected. [android:exported=true]

Description

A Service 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.

4.13 A13: Activity (de. idnow. sdk. Activities_ VideoLiveStreamActivity_ IceLink) is not Protected. [android:exported=true]

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.

Recommendation

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

4.14 A14: High Intent Priority (900) [android:priority]

Description

By setting an intent priority higher than another intent, the app effectively overrides other requests.

Recommendation

If possible, do not set higher priorities for specific intents in the manifest file.

4.15 A15: High Intent Priority (900) [android:priority]

Description

By setting an intent priority higher than another intent, the app effectively overrides other requests.

Recommendation

If possible, do not set higher priorities for specific intents in the manifest file.

4.16 A16:

Description

Evidence

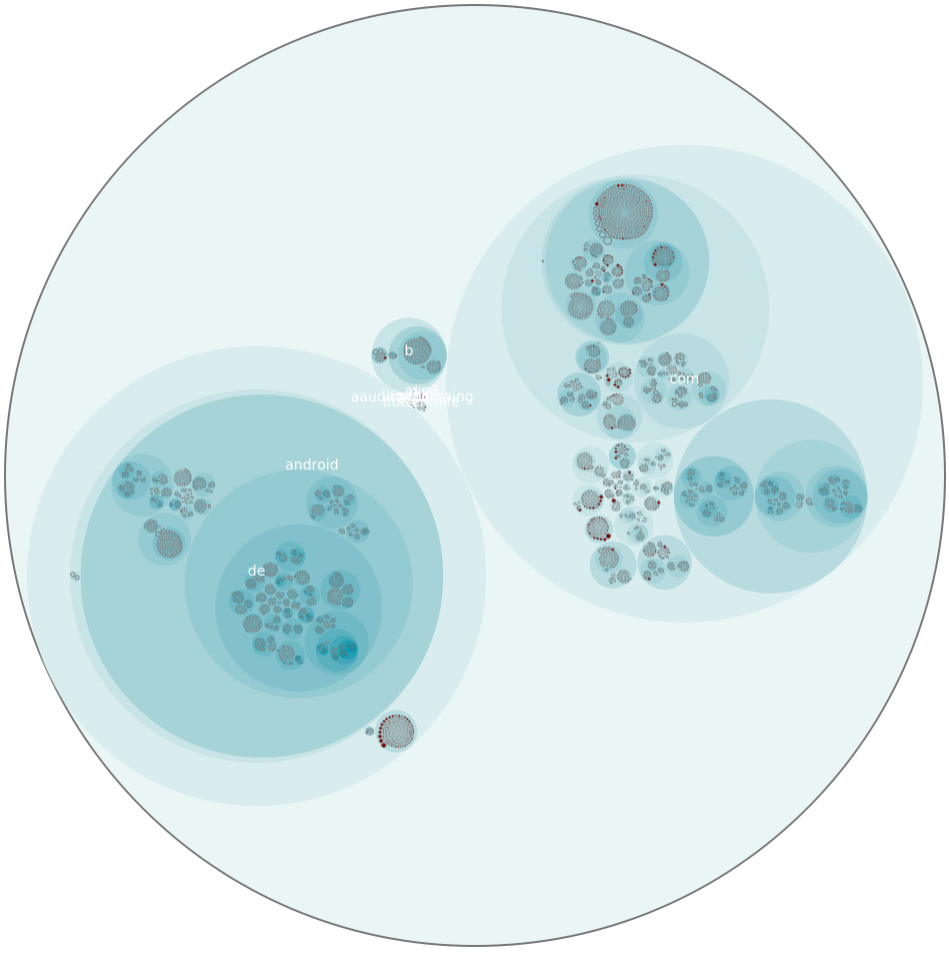
`/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/arch/lifecycle/k.smaliforName`
`/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/arch/lifecycle/k.smaligetSuperclass`
`/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/arch/lifecycle/a$b.smaliinvoke`
`/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/arch/lifecycle/a.smaligetSuperclass`
`/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/support/v4/a/e.smaliforName`
`/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/support/v4/a/e.smaliinvoke`
`/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/support/v4/a/e.smaliinvoke`
`/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/support/v4/a/f.smaliforName`
`/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/support/v4/a/f.smaliinvoke`
`/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/support/v4/a/f.smaliinvoke`
snip
For the full list view `/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/report`

Recommendation

5 VISUALIZATIONS

5.1 Chord Diagram - Class Relations

5.2 Hot Spot - System Overview



Index	Class
1	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/com/adjust/sdk/ActivityHandler.smali
2	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/de/idnow/sdk/Activities_VideoLiveStreamActivity_IceLink.smali
3	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/com/opentok/android/Session.smali
4	/home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/com/adjust/sdk/InstallReferrer.smali

5 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/de/idnow/sdk/Network_OkHttpWebSocket.smali

6 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/de/idnow/sdk/Activities_VideoLiveStreamActivity_Super.smali

7 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/support/multidex/a.smali

8 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/android/support/multidex/b.smali

9 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/com/adjust/sdk/Util.smali

10 /home/miki/Documents/GITHUB/AndroidPermissions/apks/playstore_apps/de_number26_android/app/smali/com/google/android/gms/internal/zzdvj.smali