APP漏洞扫描器之本地拒绝服务检测详解

阿里聚安全 / 2016-10-24 09:33:40 / 浏览数 4386 安全技术 漏洞分析 顶(0) 踩(0)

作者：伊樵@阿里聚安全

阿里聚安全的Android应用漏洞扫描器有一个检测项是本地拒绝服务漏洞的检测，采用的是静态分析加动态模糊测试的方法来检测，检测结果准确全面。本文将讲一下应用漏

一、本地拒绝服务产生原因和影响

Android应用使用Intent机制在组件之间传递数据，如果应用在使用getIntent()，getAction()，Intent.getXXXExtra()获取到空数据、异常或者畸形数据时没有进行异常捕获
阿里聚安全的博客以前有一篇文章《Android应用本地拒绝服务漏洞浅析》，里面详细讲了产生本地拒绝服务的四种情况：
 1、NullPointerException空数据异常：应用程序没有对getAction()等获取到的数据进行空指针判断，从而导致空指针异常而导致应用崩溃。

2、ClassCastException类型转换异常：程序没有对getSerializableExtra()等获取到的数据进行类型判断而进行强制类型转换，从而导致类型转换异常而导致应用崩溃。

3、IndexOutOfBoundsException数组越界异常：程序没有对getIntegerArrayListExtra()等获取到的数据数组元素大小的判断，从而导致数组访问越界而导致应用崩溃。
 4、ClassNotFoundException异常：程序没有无法找到从getSerializableExtra ()获取到的序列化类对象的类定义，因此发生类未定义的异常而导致应用崩溃。
当应用被恶意应用攻击时，本地拒绝服务一般会导致正在运行的应用崩溃，首先影响用户体验，其次影响到后台的Crash统计数据，另外比较严重的后果是应用如果是系统级
5曾经出现过这样的情况，它预装了一个用来测试网络连通性的系统应用，这个应用是隐藏状态，无法在桌面上打开，包名为com.lge.SprintHiddenMenu。在Android
4.4.3之前的版本里，这个应用里有大量导出的activity，这些
activity不需要任何权限就可以被外部调用。其中一个为com.lge.SprintHiddenMenu.sprintspec.SCRTN的组件是导出的，并且没有任何权限限制，给它发送一个空Intent，
5手机重启。

二、阿里聚安全扫描器的进化提升

一个简单的本地拒绝服务类漏洞，要想进行大规模的自动化扫描，扫描器也要做不少的工作，并且随着对本地拒绝服务漏洞的认识，阿里聚安全的漏洞扫描器也在不断进行优

2.1 空Intent阶段

这个阶段的扫描器是初级阶段，一般只是通过AndroidManifest.xml文件获取应用导出的组件，然后使用adb命令发送空intent给导出组件，捕获应用日志输出，查看是否有
针对空Intent导致的本地拒绝服务情况可发送如下命令测试：

```
adb shell am start -n com.jaq.dosappsample/.DosActivity
adb shell am startservice -n com.jaq.dosappsample/.DosService
adb shell am broadcast -n com.jaq.dosappsample/.DosReceiver
```

何为导出的组件？
在AndroidManifest.xml文件中如果应用的组件android:exported
属性显式指定为“true”，或者并没有显式指定为“true”也没有显式指定为“false”，什么也没有写，但是有intent-filter并指定了相应的Action，则此组件为导出的组件。

2.2 解析Key值阶段

空Intent导致的拒绝服务毕竟只是一部分，还有类型转换异常、数组越界异常等导致的本地拒绝服务。在解析Key值阶段扫描器需要分析组件代码中是否使用了一些关键函数
在Activity组件中的onCreate()方法中，Service组件中的onBind()和onStartCommand()方法中，BroadcastReceiver组件的onReceive()方法中，如果组件没有做好权限控
catch异常保护，如果没有则会有本地拒绝服务风险。
在这一阶段扫描器遇到的挑战是找到这些关键函数中的Key值，Action值，不仅要找到，还要找到key对应的类型，来组装adb命令，发送命令给安装好的应用进行测试。

2.3 通用型拒绝服务阶段

2015年年初的时候，业界又爆出了通用型拒绝服务，由于应用中使用了getSerializableExtra()
的API，应用开发者没有对传入的数据做异常判断，恶意应用可以通过传入序列化数据，导致应用本地拒绝服务。此种方法传入的key值不管是否与漏洞应用相同，都会抛出类
针对这个常用的手工检测POC代码如下：

此阶段扫描器遇到的难题是无法直接通过adb命令进行测试，因为无法用adb命令传递序列化对象给应用。业界大部分漏洞扫描器也因为无法发送序列化对象给应用都止步解

2.4 动态注册BroadcastReceiver阶段

BroadcastReceiver组件一般分为两种，一种是静态注册，提前在AndroidManifest.xml声明组件；另外一种是动态注册，在代码中使用registerReceiver()方法注册Broadc
动态注册BroadcastReceiver的常见使用方法如下：

很多开发者没有意识到，如上使用registerReceiver()方法注册的是全局BroadcastReceiver，和静态注册BroadcastReceiver
android:exported属性为true性质一样，如果没有指定权限访问控制（permission参数），可以被任意外部应用访问，向其传递Intent，根据具体情况产生的危害可能不同
动态注册BroadcastReceiver导致导出的Receiver这种情况非常少被大家注意，现有的一些安全检测工具、扫描器都不能发现动态注册的BroadcastReceiver。在此阶段，动
通过阿里聚安全的漏洞扫描器对一些样本进行了检测，也发现了不少动态注册BroadcastReceiver导致的本地拒绝服务攻击。

三、本地拒绝服务漏洞现状

为了了解本地拒绝服务漏洞的现状，阿里聚安全的应用漏洞扫描器针对国内外的各行业主要APP进行了扫描，共扫描了三百多款APP。
国内行业主要是通过采集国内某应用市场的APP，我们采集了各个行业的TOP

APP总共有151个，发现拒绝服务漏洞的总个数为970个，平均个数为6.4个，其中影音播放类的APP本地拒绝服务个数最多，健康类安全类和运营商类比较少、游戏类的最少
国内行业APP本地拒绝服务漏洞情况：

柱状图是国内各个行业APP按本地拒绝服务漏洞平均个数排序：

下图是各个组件引起的本地拒绝服务的数量、占比情况：

国内行业动态注册BroadcastReceiver导致的本地拒绝服务漏洞有247个，约占拒绝服务漏洞总数的25%，比静态注册BroadcastReceiver的要多不少：

国外行业主要是通过采集Google Play上的APP，我们也采集了各个行业的TOP
APP总共有177个，发现拒绝服务漏洞的总个数是649个，平均漏洞个数为3.7个，平均漏洞个数最多的是办公类应用，最少的和国内行业一样是游戏。
国外行业APP本地拒绝服务漏洞情况：

国外各个行业的应用本地拒绝服务漏洞平均个数排序：

各个组件引起的本地拒绝服务的数量、占比情况：

国外行业动态注册BroadcastReceiver导致的本地拒绝服务漏洞有147个，约占拒绝服务漏洞总数的23%，比国内的情况略少，可见动态注册BroadcastReceiver导致的本地

总体上来看，本地拒绝服务风险因为具有Android版本无关性，漏洞本身对APP影响也不大，只与应用开发者是否注意、重视有关，所以现在还经常在应用中出现。在各大厂

四、阿里聚安全对开发者建议

（1）阿里聚安全的漏洞扫描器已经具备覆盖动态注册Receiver产生的拒绝服务漏洞（目前，还没发现友商的漏洞扫描器有这样的能力），使用阿里聚安全的漏洞扫描器进行
（2）不必要导出的组件将其exported属性显式的设为“false”，这样可以减少应用的攻击面。
（3）导出的组件在getIntent()后，Intent.getXXXExtra()时用try…catch做好异常处理。
（4）在导出的组件设置好权限控制，不让任意第三方应用访问。
（5）对于动态注册的BroadcastReceiver，尽量少用registerReceiver()方法，如果只在本应用内通信，改用LocalBroadcastManager的registerReceiver()进行本地注册，

五、参考

1、Android
APP通用型拒绝服务漏洞分析报告，http://blogs.360.cn/blog/android-app%E9%80%9A%E7%94%A8%E5%9E%8B%E6%8B%92%E7%BB%9D%E6%9C%8D%E5%8
2、Android应用本地拒绝服务漏洞浅析，https://jaq.alibaba.com/blog.htm?id=55
3、https://developer.android.com/guide/components/activities.html
4、https://developer.android.com/guide/components/services.html
5、https://developer.android.com/reference/android/content/Context.html
6、https://labs.mwrinfosecurity.com/advisories/2014/11/05/nexus-5-4-4-2-local-dos/

作者：伊樵@阿里聚安全，更多Android、iOS安全文章,请访问阿里聚安全官网