Android安全开发之启动私有组件漏洞浅谈

阿里聚安全 / 2017-04-06 09:13:49 / 浏览数 3431 安全技术 技术讨论 顶(0) 踩(0)

0x00 私有组件浅谈
android应用中，如果某个组件对外导出，那么这个组件就是一个攻击面。很有可能就存在很多问题，因为攻击者可以以各种方式对该组件进行测试攻击。但是开发者不一定
□
对于这样的问题，最方便的修复方式就是在确定不影响业务的情况下，将这个存在问题的组件不对外导出变成私有组件。这样做的确很有效，私有组件也很安全。但是，如果
正常情况：

私有组件能被启动情况：

0x01 启动私有组件原理分析
存在一个私有组件A，和一个对外导出组件B。如果B能够根据对外传入的Intent中的内容打开私有组件A，同时启动私有组件A的Intent的内容来自启动导出组件B的Intent的

下面用一个简单例子来说明如果能够启动私有组件，能引起的一些安全问题。
PrivateActivity.class

很明显，PrivateActivity是存在问题的，因为从Intent中直接获取值之后，没有做任何异常处理。如果PrivateActivity是私有的一个Activity，并且开发工程师能保证传入到该

那么，攻击者就可以通过着么一条命令去实施攻击：

那么应用就会崩溃。

这里只是一个简单的demo，用来说明存在问题。如果PrivateAcitivty里面存在很重要的逻辑业务处理的话，那么恶意攻击者可以通过控制MainActivity去控制PrivateActivi

除了以上这种情况之外，还有一种情况，就是Intent Scheme
URL，如果处理不当的话，也极有可能通过解析Uri的这个导出的组件去攻击启动其他私有组件。本质都是一样的，这里就不讨论这种情况了。

0x03 启动私有组件案例分析
这里以某个app7.5.0版本为例，分析它因为可以启动私有组件导致的严重问题。（目前该app已经没有再使用有问题的组件，有问题的SDK也早已经修复了这个问题）
首先，这个app存在一个私有组件VersionUpdateActivity：

这个私有组件是用来判断是否更新的，如果有，会根据Intent中的url链接去下载相应的更新apk包。
另外，该apk存在另外一个对外导出的组件。

该组件在实现过程中，通过获取到的Intent，经过一系列检查，进入pushClickedResult函数中。

在pushClickedResult函数中，主要做了以下几个操作：
1、首先获取intent中activity
2、然后将这个值作为将要启动的activity的classname
3、将intent传入将要启动的activity
4、然后启动activity

那么很明显了，攻击者可以通过控制XGPushActivity进而控制这个应用的所有私有activity。
攻击私有组件VersionUpdateActivity的POC如下：

这个命令会打开VersionUpdateActivity，如果存在更新，那么点击更新，下载的将是url对应的内容。

0x04 阿里聚安全对开发者的建议
首先，阿里聚安全已经能够检测到这样的问题了。对于上面案例分析中的app，阿里聚安全扫描器扫描到的结果如下：

对于这样的安全风险，阿里聚安全建议：
1、对于不必要对外导出的组件，请设置exported=false。
2、如果该组件因为各种原因，需要导出，那么请检查该组件能不能根据该组件的intent去启动其他私有组件。如果能，请根据业务严格控制过滤和校验intent中的内容，同时

阿里聚安全 | Android安全开发系列文章
Android安全开发之安全使用HTTPS
Android安全开发之通用签名风险
Android安全开发之ZIP文件目录遍历
Android安全开发之Provider组件安全
Android安全开发之浅谈密钥硬编码
Android安全开发之浅谈网页打开APP
Android应用安全开发之浅谈加密算法的坑

• 作者：舟海、呆狐@阿里聚安全，更多阿里安全类技术文章，请访问阿里聚安全官方博客：https://jaq.alibaba.com/community/index.htm

上一篇：Drupal 7.x Servic... 下一篇：双剑合璧-Linux下密码抓取神器...

1. 1 条回复

 hades 2017-04-10 04:59:26

就是那么的专业 这系列很赞

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板