有朋友聊天，我才想起来这篇预警。

这个漏洞非常凶残，使用J2EE框架的，基本都被X了。只要是个J2EE的网站，这个漏洞必须打补丁，否则等死。

从时间上看，阿里巴巴的框架第一个修补漏洞。

http://openwebx.org/forum/showthread.php?tid=634

不知道各位的CPU满过没有，如果没有满，往这里来：

http://www.exploit-db.com/exploits/31615/

**J2EE框架DDoS漏洞预警**

**已确认被成功利用的软件及系统：**

大部分常见J2EE WEB框架

STRUTS1全版本（只影响使用uploadform的action）

STRUTS2全版本（任何一个action都受影响）

Spring MVC全版本（任何一个controller都受影响）

所有使用了apache commons fileupload的组件的应用，包括纯JSP页面

Commons FileUpload 1.0 to 1.3

部分服务器自带了upload组件，可以直接让JSP调用

Apache Tomcat 8.0.0-RC1 to 8.0.1

Apache Tomcat 7.0.0 to 7.0.50

JBOSS由于重用tomcat源码所以受到影响

**漏洞描述：**

Apache Commons FileUpload 1.3在处理mime-multipart请求时，攻击者可以构造一个包含异常http头的请求，使得apache fileupload进入无限循环，导致CPU爆满，拒绝服务。

漏洞分析这次就不发了，原理太简单，就是个循环无法退出。

PID   COMMAND   %CPU

8070   mdworker     1.3

8069   sleep           0.0

8066   top             11.2

8064   java            101.2

这个漏洞可以用于攻击大多数J2EE框架，常见J2EE框架，总会默认使用FileUpload组件，并且在所有用户代码前完成上传文件的预处理，这导致无论开发者是否手工调用该组件，都会默认执行。

此漏洞的POC已经被攻击者发布，请尽快修补该问题，以免造成损失。

ps：如果运维过程中，发现CPU无故飙升，可以优先考虑这个因素。

**修补方案：**

升级Apache Commons FileUpload 1.3.1 或之后版本

升级Apache Tomcat 8.0.2 或之后版本

升级 Apache Tomcat 7.0.51 或之后版本

http://markmail.org/message/kpfl7ax4el2owb3o

http://tomcat.apache.org/security-8.html

http://tomcat.apache.org/security-7.html