# 安全小课堂第五十一期【Struts2漏洞原理讲解】

京东安全应急响应中心 2017-03-31

Struts2是一种web开发框架，当前被广泛应用到大型互联网企业、政府及金融机构的网站建设中。由于Struts2 对底层性导致整个web系统对其安全性的依赖程度很高。近期，Apache公司公布了Struts2的两个安全漏洞，引起业界的高度重视。JSRC **安全小课堂第五十一期**，我们邀请到了**Tony**、**恋锋**师傅分享一下Struts2漏洞原理、危害及修复方案,以及 JSRC 白帽子们的精彩讨论。

**讲师：Tony**

讲师简介：

唯品会高级信息安全工程师，近5年安全行业从业经验。精通web安全，企业安全,对移动安全和二进制也有一定了解，熟悉JAVA，Python。目前从事代码评审，JAVA安全框架防御研究工作。

**讲师：恋锋**

讲师简介：

网络尖刀成员，JSRC白帽子，具备多年信息安全从业经历，在应用安全领域有较深的研究。

**S2-045与S2-046漏洞的危害?**

京安小妹

官方评级该类漏洞为高危，也是一种0day,并不需要找个上传的地方只需要模拟上传发包。其中的jakarta解析器是Struts 2框架的标准组成部分。默认情况下jakarta是启用的，所以该漏洞的严重性需要得到正视。

执行任意命令，上传shell等危害。

讲师：Tony、恋锋

**S2-045与S2-046漏洞的原理，具体出现问题的原因?**

京安小妹

主要是Struts2默认文件上传解析器jakarta的使用。
S2-045漏洞原因：基于Jakarta Multipart parser的文件上传模块在处理文件上传(multipart)的请求时候对异常信息做了捕获，并对异常信息做了OGNL表达式处理。但在在判断content-type不正确的时候会抛出异常并且带上Content-Type属性值，可通过精心构造附带OGNL表达式的URL导致远程代码执行。
S2-046成因与S2-045比较相似，通过使用恶意的Content-Disposition值或者使用不合适的Content-Length头就可能导致远程命令执行。
S2-045:
struts.multipart.parser=jakarta（/org/apache/struts2/default.properties）
Content-Type的解析错误
Content-Type包含OGNL表达式
S2-046:
<constant name="struts.multipart.parser" value="jakarta-stream" />
http请求头中的 Content-Length 需要大于 2097152
文件名包含 OGNL 表达式。
都是在处理error消息的时候触发,把包含OGNL表达式的content-TYPE或filename解析执行了。

讲师：Tony、恋锋

**为什么说S2-045与S2-046漏洞实际上是同一个漏洞呢?**

京安小妹

两者攻击点相同，都是因为使用的Jakarta插件造成的，只是攻击维度不同（S2-045利用位置是Content-Type，S2-046利用位置是Content-Dispostion / Content-Length）。
都是文件上传解析器jakarta的使用。
都是error消息的处理，只是error的点不一样，一个是content-type，一个是content-length。
触发命令执行函数都是LocalizedTextUtil.findText();
s2-046触发异常是因为文件大小超过规定，S2-045是content-TYPE。

讲师：Tony、恋锋

**白帽子提问:推荐检测工具有哪些?**

检测工具github上有很多了。
直接搜索S2-045或S2-046能找到不少。
apache官方也有公开的poc进行检测。
白帽子也开源了不少检测poc。

讲师：Tony、恋锋

**白帽子提问:S2-045-046 getshell的方法?**

只要达到触发异常条件，把shellcode注入到content-type与filtename就行了。

讲师：Tony、恋锋

**S2-045与S2-046漏洞与之前Struts2框架漏洞有何异呢?**

京安小妹

Struts2漏洞的根源基本都是对OGNL表达式的解析执行。

struts2标签使用了OGNL表达式，OGNL表达式使用表达式语法导航对象图。功能强大，可以访问后端对象或类的方法，属性。

不同点在于这次是发生在对error消息的处理中，以前一般都有一个直接的OGNL表达式注入点。

利用无需任何前置条件（debug等功能）以及启用任何插件。

Struts2框架漏洞的类型有很多，apache官网累积已发布46个struts框架漏洞，涉及到xss、文件遍历、CSRF攻击、远程命令执行等，其中命令执行类漏洞最多。像S2-045与S2-046漏洞就属于命令执行类漏洞。

以前有些漏洞有前置条件,比如开启debug模式等等，所以这次危害比较大。

讲师：Tony、恋锋

**如何检测S2-045与S2-046漏洞?**

京安小妹

现在批量扫描的工具也很多,struts2-core.x.x.jar的版本号。
内部检查，check下框架版本。
目前互联网上有不少验证该类漏洞的poc，可直接使用。

讲师：Tony、恋锋

**如何修复S2-045与S2-046漏洞?**

京安小妹

更新版本,升级至安全版本。
更新到 Struts 2.3.32 or Struts 2.5.10.1。
针对struts2 0day漏洞刚出来的时候也可以采用一些临时防御措施，针对POC字段，在waf上面或者应用本身添加filter。
严格过滤 Content-Type 、filename里的内容，严禁ognl表达式相关字段。
删除commons-fileupload-x.x.x.jar文件，不过文件上传不可用。

讲师：Tony、恋锋

**白帽子提问:struts2-045、046的POC构造?**

POC的构造有很多啊。看下POC代码，或工具发包的时候抓包看下。
调试的话，搭建环境，在struts2的入口类打断点就好。

讲师：Tony、恋锋

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，回复“安全小课堂”或者点击阅读原文进行查看。

**最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。**

**简历请发送：cv-security@jd.com**

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心

阅读原文