



开源资讯

当前位置：  
综合资讯 » **Struts** ， 投递新闻»

资讯、软件、分享、代码、博客

搜索

## 灾难日：中国互联网惨遭Struts2高危漏洞摧残

疯狂的艺术家 发布于：2013年07月18日 ([140](#)评)

分享到 新浪微博 腾讯微博

收藏 +41

Struts是Apache基金会Jakarta项目组的一个开源项目，Struts通过采用Java Servlet/JSP技术，实现了基于Java EE Web应用的Model-View-Controller（MVC）设计模式的应用框架，是MVC经典设计模式中的一个经典产品。目前，Struts广泛应用于大型互联网企业、政府、金融机构等网站建设，并作为网站开发的底层模板使用，是应用最广泛的Web应用框架之一。

Struts

近日，Struts2曝出2个高危安全漏洞，一个是使用缩写的导航参数前缀时的远程代码执行漏洞，另一个是使用缩写的重定向参数前缀时的开放式重定向漏洞。这些漏洞可使黑客取得网站服务器的“最高权限”，从而使企业服务器变成黑客手中的“肉鸡”。

Apache Struts团队已发布了最新的Struts 2.3.15.1，修复了上述漏洞，建议采用Struts 2.0至Struts 2.3的网站开发者尽快升级至最新版。

据乌云平台漏洞报告，淘宝、京东、腾讯等大型互联网厂商均受此影响，而且漏洞利用代码已经被强化，可直接通过浏览器的提交对服务器进行任意操作并获取敏感内容。Struts漏洞影响巨大，受影响站点以电商、银行、门户、政府居多，而且一些自动化、傻瓜化的利用工具开始出现，填入地址可直接执行服务器命令，读取数据甚至直接关机等操作。

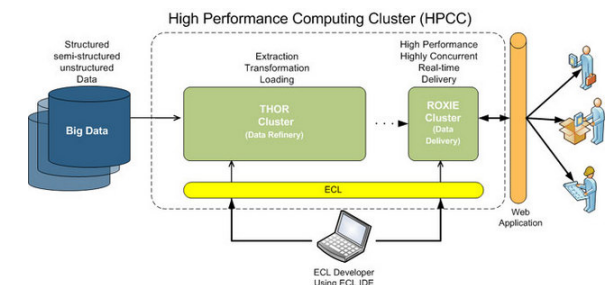
灾难日：中国互联网惨遭Struts2高危漏洞摧残

租服务器 上51IDC

上海BGP 650元起

本周推荐 HPCC Systems

HPCC (High Performance Computing Cluster) 是一个大规模并行处理计算平台，用于解决大数据问题。类似 Hadoop 平台。



2. 迷你PC平台 [pcDuino](#) »
3. 开源虚拟化解决方案 [XenServer](#) »
4. 企业虚拟化平台 [CecOS](#) »

# 安全预警：Struts2框架远程命令执行漏洞

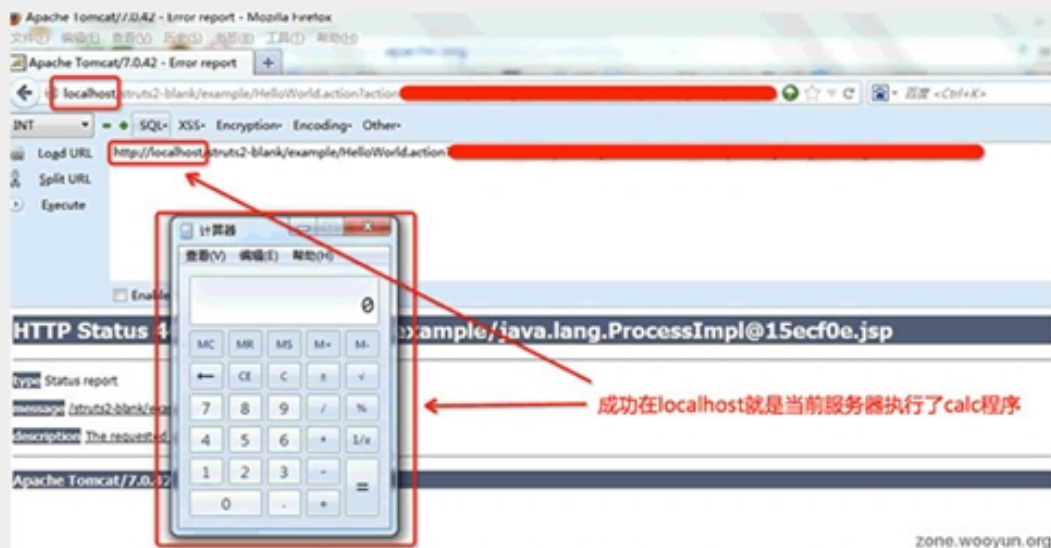
漏洞作者：N/A 相关厂商：Apache 缺陷编号：Zone-5159

## 1, 官方公告

<http://struts.apache.org/release/2.3.x/docs/s2-016.html>

<http://struts.apache.org/release/2.3.x/docs/s2-017.html>

2, 本次涉及的安全漏洞s2-016, s2-017影响所有版本(2.0-2.3.15), 涉及漏洞可在当前服务器上执行任意命令或访问重定向。



## 5. iOS游戏引擎 Sparrow Framework »

[更多以往推荐 »](#)

### 本周热点资讯

- 灾难日：中国互联网惨遭Struts2... 14小时前
- 程序员最怕的事 4天前
- Linux 不为人知的12大内幕 3天前
- 超过 30 款免费的扁平风格图标集... 5天前
- Windows 操作系统垄断地位崩塌... 22小时前
- 做正确的事情，等着被开除 3天前
- Chrome 29 新功能一览 昨天(10:18)
- 内核开发者呼吁 Linus Torvalds... 昨天(8:28)
- 甲骨文将停止开发 Sun 虚拟化技... 昨天(8:39)
- 我在 Facebook 的这三年 昨天(8:35)

### 本站最新资讯

- Google 请放心 Facebook 搜索不... 4分钟前
- Wine 1.6 发布，Windows 模拟器... 9分钟前
- #翻译# 树莓派的硬件随机数生成... 13分钟前
- Rails: 只在需要的时候加载需要... 14分钟前
- 【每日一博】CloudStack 4.1.0 ... 16分钟前
- fastjson-1.1.34版本发布，修复... 9小时前
- 灾难日：中国互联网惨遭Struts2... 14小时前
- Rikulo UI 0.6.8 发布，支持最新... 15小时前
- Linux支持运行Direct3D 9游戏，... 17小时前
- 7 款免费的 Metro UI 模板... 19小时前

```

tcp      0      0 127.0.0.1:1098      0.0.0.0:*           LISTEN
tcp      0      0 127.0.0.1:21098     0.0.0.0:*           LISTEN
tcp      0      0 0.0.0.0:60939       0.0.0.0:*           LISTEN
tcp      0      0 127.0.0.1:1099      0.0.0.0:*           LISTEN

```

4, 目前官方发布版本2.3.15.1来修复这两个安全漏洞, 请运维人员速度更新!

The Apache Software Foundation  
http://www.apache.org/  
Published: 2013-07-16

## Struts™

Apache | Struts 2 | Struts 1 (EOL)

### Apache Struts 2.3.15.1 GA

Released on 16 July 2013. The version notes are available online. Scroll down for more about Apache Struts, the Apache Struts project, and Struts for Newbies

[Download](#) [Read more](#)

### Apache Struts 1 End-Of-Life (EOL)

The Apache Struts Project Team would like to inform you that the Struts 1.x web framework has reached end of life and is no longer officially supported.

[Read more](#) [Press release](#)

5, 目前乌云已经接到大量互联网企业漏洞报告, 包括京东、淘宝、腾讯等。

提交日期	漏洞名称	评论/关注	作者
2013-07-17	PHPCMS V9 鸡肋注入漏洞	0/0	tenzy
2013-07-17	百度某分站最新Struts命令执行漏洞一枚	3/2	波波虎
2013-07-17	腾讯某业务struts2命令执行	7/12	erevus
2013-07-17	京东商城几处struts2命令执行漏洞	2/5	梧桐雨
2013-07-17	淘宝某分站最新Struts命令执行漏洞第二枚	3/7	print
2013-07-17	国美最新struts2命令执行漏洞	0/1	erevus
2013-07-17	淘宝某分站最新Struts命令执行漏洞一枚,可执行系统命令	10/15	Finger
2013-07-17	腾讯微博可钓鱼+成功案例~	8/9	Nicky
2013-07-17	站将网设计缺陷导致任意用户密码可重置	1/2	herOma
2013-07-17	众多天猫商城官方旗舰店管理不当导致资料泄露 (nuk 卓众车品专营店等)	0/2	...相遇...
2013-07-16	百合网某分站源码下载导致服务器沦陷	1/7	heiren...

最后再次提醒广大网站管理员, 尽快将Struts 2升级到最新的2.3.15.1版本。

Struts 2.3.15.1官方下载: <http://struts.apache.org/download.cgi#struts23151>

Everything you need to build  
HTML5 sites & mobile apps

Kendo UI

Free Download

Struts 的详细介绍：[请点击这里](#)

Struts 的下载地址：[请点击这里](#)

想通过手机客户端访问开源中国：[请点击这里](#)

本文转载自：驱动之家  
(本站只作转载,不代表本站同意文中观点或证实其文中信息)

旧一篇：[Rikulo UI 0.6.8 发布，支持最新的 Dart SDK](#) 12小时前

新一篇：[fastjson-1.1.34版本发布，修复不兼容问题](#) 6小时前


相关资讯

- [Apache Struts2 再发布漏洞修复版本...](#) 1个月前
- [Struts2 安全更新版本发布，请尽快升...](#) 1个月前
- [Fastupload 0.4.7 发布，支持 stru...](#) 8个月前
- [【每日一博】Struts2 请求处理流程及...](#) 10个月前
- [Struts2 2.3.3发布](#) 1年前
- [方便struts2项目调试 - ConfigDebu...](#) 2年前
- [struts2调试插件-configdebug...](#) 2年前
- [Struts2 jQuery Plugin 3.0 的新特性...](#) 2年前

相关讨论话题

- [我这样能值多少？](#) 13小时前
- [谁公司用的struts2，没升级的，给个...](#) 15小时前
- [struts2暴远征命令执行漏洞](#) 昨天(20:43)
- [2013年07月17日 Struts2远程执行命令...](#) 18小时前
- [Struts2的默认执行方法execute和方法...](#) 昨天(23:37)
- [struts2.3.15 注解注入](#) 昨天(15:13)
- [JAVA三年工作以后的简历,有什么不足...](#) 4个月前
- [struts2里的action方法里怎么访问w...](#) 1年前
- [weblogic不支持struts2吗...](#) 10天前
- [javascript中使用Struts2的标签获取...](#) 1年前

网友评论，共 140 条 [发表评论](#) [回到顶部](#)

 1楼：**ddatsh** 发表于 2013-07-18 16:18 [回复此评论](#)  
所以不懂技术不关心安全的，被虐很正常  
技术好点的，很多可能不用Struts的





2楼：戴威 发表于 2013-07-18 16:18 [回复此评论](#)

spring-mvc飘过



3楼：心中的日月 发表于 2013-07-18 16:20 [回复此评论](#)

引用来自“戴威”的评论

spring-mvc飘过

一样，哈。



4楼：颜\_ 发表于 2013-07-18 16:20 [回复此评论](#)

很严重...



5楼：wenshao 发表于 2013-07-18 16:21 [回复此评论](#)

引用来自“戴威”的评论

spring-mvc飘过

spring-mvc一样暴过两次远程代码执行漏洞



6楼：hanQ 发表于 2013-07-18 16:21 [回复此评论](#)

Struts2Exp.jar 笑而不语 [@Track3r](#)



7楼：酒逍遥 发表于 2013-07-18 16:23 [回复此评论](#)

看来java的安全性也不比php 高太多啊...

以后谁再说 java安全性比php 高就拿 这个喷死它



8楼：gosu 发表于 2013-07-18 16:23 [回复此评论](#)

struts开发者对这漠视的很。



9楼：JayKong 发表于 2013-07-18 16:23 [回复此评论](#)

楼下开喷！



10楼：mmppp33 发表于 2013-07-18 16:23 [回复此评论](#)

java 悲剧了



11楼：IdleMan 发表于 2013-07-18 16:24 [回复此评论](#)

数据盗完后，觉得太无聊，再写几个傻瓜工具供大众娱乐



12楼：超级大富 发表于 2013-07-18 16:26 [回复此评论](#)

引用来自“酒逍遥”的评论

看来java的安全性也不比php高太多啊...

以后谁再说java安全性比php高就拿这个喷死它

这个又不代表Java Web，只能是很小一部分，OSChina也是Java写的。



13楼：Qbase 发表于 2013-07-18 16:27 [回复此评论](#)

该盗的都被盗了！现在才发补丁。



14楼：王涛 发表于 2013-07-18 16:28 [回复此评论](#)

框架啊，表达式语言啊



15楼：sikele 发表于 2013-07-18 16:28 [回复此评论](#)

引用来自“ddatsh”的评论

所以不懂技术不关心安全的，被虐很正常

技术好点的，很多可能不用Struts的

那用什么？SSH2不是标配么？



16楼：sikele 发表于 2013-07-18 16:29 [回复此评论](#)

用asp.net mvc的路过。。



17楼：王涛 发表于 2013-07-18 16:30 [回复此评论](#)

引用来自“超级大富”的评论

引用来自“酒逍遥”的评论

看来java的安全性也不比php高太多啊...

以后谁再说java安全性比php高就拿这个喷死它

这个又不代表Java Web，只能是很小一部分，OSChina也是Java写的。

osc高明之处在于[@红薯](#) 没用各种表达式语言来解析字符串并执行



18楼：luciferdragon 发表于 2013-07-18 16:30 [回复此评论](#)

因为使用java的相对比较多获得利益的可能性相对较大所以被人针对的更严重，就像windows的操作系统一样，用的人多研究系统漏洞的人就多，现在用android的人多了，研究java漏洞的当然会增多。你能想象塞班系统的漏洞还

有人去研究吗。。。没有市场研究出来自娱自乐吗。。



19楼：**RuralHunter** 发表于 2013-07-18 16:31 [回复此评论](#)

引用来自“**sikele**”的评论

引用来自“**ddatsh**”的评论

所以不懂技术不关心安全的，被虐很正常

技术好点的，很多可能不用Struts的

那用什么？SSH2不是标配么？

你的标配，不要放到别人身上。SSH这3个我一个都不会是不是很奇葩？



20楼：**Hello-Java** 发表于 2013-07-18 16:31 [回复此评论](#)

引用来自“超级大富”的评论

引用来自“酒逍遥”的评论

看来java的 安全性 也不比php 高太多啊...

以后谁再说 java安全性比php 高就拿 这个喷死它

这个又不代表Java Web，只能是很小一部分，OSChina 也是Java 写的。

是的，这个漏洞的和语言没有关系。如果有个框架允许http提交的参数当成系统命令进行调用，那么不管什么语言的http server都会有这个漏洞

1

2

3

4

5

6

7

>

网名： (必填)

邮箱： (必填，不公开)

网址：

验证码：



[换另外一个图](#)

发表评论

与内容无关的评论将被删除，严重者禁用帐号

[回到顶部](#) [回到评论列表](#)

你也许会喜欢

- ▣ [Apache Struts2 再发布](#)
- ▣ [Struts2 安全更新版本发](#)
- ▣ [Fastupload 0.4.7 发布](#)