i春秋实验--struts2远程命令执行S2-045漏洞利用与修复

转载

weixin_30949361 于 2017-03-12 16:32:00 发布 167 收藏 1
文章标签： java 运维
原文链接：http://www.cnblogs.com/solozhou/p/6538285.html

实验环境

操作机：Windows XP

目标机：CentOS 6.5

实验目的

了解S2-045 Struts2远程命令执行漏洞的危害

掌握检测修复S2-045 Struts远程命令执行漏洞技术

实验内容

Apache Struts 2被曝存在远程命令执行漏洞，漏洞编号S2-045，CVE编号CVE-2017-5638，在使用基于Jakarta插件的文件上传功能时，有可能存在远程命令执行，导致系统被黑客入侵。

恶意用户在上传文件时通过修改HTTP请求头中的Content-Type值来触发该漏洞，进而执行系统命令。

影响范围

Struts 2.3.5 --Struts 2.3.31

Struts 2.5 --Struts 2.5.10

不受影响的范围

Struts 2.3.32 Struts 2.5.10.1

快速检测方式

使用知道创宇SeeBug照妖镜可以直接检测该站点是否存在漏洞。

漏洞危害

在default.properties文件中，struts.multipart.parser的值有两个选项分别是jakarta和pell。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得到正视。

攻击者可以通过远程命令注入执行，另系统执行恶意命令，导致黑客入侵，从而威胁服务器安全，影响极大。

实验步骤

步骤一：验证漏洞

打开目标网站：http://172.16.12.2/

发现目标网站跳转至：http://172.16.12.2/example/HelloWorld.actiond

打开cmd并切换至poc.exe所在目录，执行下列命令：

```
poc.exe http://172.16.12.2/example/HelloWorld.action "ifconfig"
```

成功执行，说明漏洞存在。可以尝试其他命令：

```
poc.exe http://172.16.12.2/example/HelloWorld.action "cat /etc/passwd"
```

步骤二：修复漏洞

修改Struts2的Multipart parser

1，使用ssh登陆到目标主机172.16.12.2，用户名root，密码123456

2，将struts2-core-2.3.31.jar（路径：/var/www/apache-tomcat-7.0.14/webapps/ROOT/WEB-INT/lib/）下载到桌面，修改文件扩展名为struts2-core-2.3.31.zip，解压并打开文件夹org\apache\struts2。

编辑struts.multipart parser文件，该选项就是Struts2的Multipart parser应用配置，默认值是jakarta，即此次出现命令执行漏洞的上传框架。

将其修改为pell，相当于将存在漏洞的jakarta框架禁用了。

修改值struts.multipart parser,保存,退出。（在struts.multipart parser=jakarta前加上#，去掉struts.multipart parser=pell前面的#）

3，重新打包.jar文件

在struts2-core-2.3.31文件夹全部选中，压缩打包为struts2-core-2.3.31.jar

4，替换.jar文件

使用SSH工具中的Xftp，将原有的文件mov至/目录，将新打包的文件放到该目录下。

5，重启tomcat

```
1 cd /var/www/apache-tomcat-7.0.14/bin
2 ./shutdow.sh
3 ./startup.sh
```

6，漏洞验证

```
poc.exe http://172.16.12.2/example/HelloWorld.action "ifconfig"
```

此时poc程序已无法成功利用了。

转载于:https://www.cnblogs.com/solozhou/p/6538285.html