登录

Struts2_048(CVE-2017-9791)远程代码执行漏洞EXP

killshadow / 2017-12-29 00:37:16 / 浏览数 4909 安全技术 漏洞分析 顶(0) 踩(0)

一、漏洞分析

1. 漏洞背景：

官方说明：

> It is possible to perform a RCE attack with amalicious field value when using the Struts 2 Struts 1 plugin and it's a Struts1 action and the value is a part of a message presented to the user, i.e. whenusing untrusted input as a part of the error message in the ActionMessageclass.

详见：https://cwiki.apache.org/confluence/display/WW/S2-048
这个漏洞本质上是在struts2-struts1-plugin这个jar包上。这个库是将struts1的action封装成struts2的action以便在strut2上使用。

主要受影响的Struts版本为：2.3.x

攻击者构造恶意字段值（value）通过Struts2的struts2-struts1-plugin传递给被攻击主机，从而实现RCE，获取远程主机的控制权限。

2. 漏洞原因

showcase/src/main/java/org/apache/struts2/showcase/integration/SaveGangsterAction.java下，“Struts1.gangsterAdded”被引入：

showcase/src/main/resources/globalMessages.properties下“Struts1.gangsterAdded”被定义. Struts1.gangsterAdded是一个关键值，一旦“Gangster{0} added successfully”，它将绕开执行OGNL代码。

这个漏洞本质上是在struts2-struts1-plugin这个jar包上。这个库是将struts1的action封装成struts2的action以便在strut2上使用。本质问题出在struts2-struts1-plugin

输入参数之后，执行Struts1ction的execute方法。

调用saveGangsterAction的excute方法，将表单中地内容封装到actionforward，这个方法中就带入有毒参数gforn.getName()放到了messages结构中，gform.getNa

攻击者将用户可控地值添加到ActionMessage并在客户前端展示，导致其进入getText函数，最后messageb被当作ognl表达式执行。以下两部分代码事位于integration app下的SaveGangsterAction.java部分源码：

3.漏洞总结：

通过运行struts1Acion.java的execute方法，获取Action。

调用saveGangsterAction的execute方法，这部分代码就是漏洞代码，这里创建了一个action message变量，将表单请求封装到actionForm中。代码详见图2.6）

设置标识，获取ActionMessage。

回到Struts1Action.java，跟着代码流，我们能看到控制流到达getText方法在TextProviderSupport.java：红框所示的是在LocalizeTextUtil.Java中FindText的方法。这

如果这种方法在提供地key中没有找到message，它就会调用getDefaultMessage地方法：

translateVariables方法从OgnlTextPrasrt.java中调用parser.evaluate方法,Parser.evaluate函数事负责从message段中解析OGNL表达式的，它检查在message中的“${

在Apache Struts中，大部分OGNL注入漏洞都被爆出来了。攻击者能够利用这些漏洞很容易就执行命令，因为OGNL注入漏洞比起其他攻击更简单。

漏洞防护：1）停用Struts2-struts1-plugin插件、showcase.war；2）讲直接传递原始值改为使用资源键：

二、宿主环境及攻击环境

这里，我开了两个虚拟机，kali做攻击机，Centos做靶机，以模拟RCE。

1. 靶机：centOS 7.3：
2. 攻击机：kali linux

三、EXP实现

1.搭建漏洞环境

下载漏洞环境包：http://archive.apache.org/dist/struts/2.3.24/struts-2.3.24-apps.zip

下载Tomcat：http://tomcat.apache.org/tomcat-7.0-doc/index.html

在Centos解压Tomcat包（这里我解压到用户目录下）

将下载好的漏洞环境包解压，将struts2-showcase.war，将移至解压后的Tomcat目录下的webapps下

开启Tomcat，执行命令：

2.本地验证漏洞

在终端打开Tomcat之后，在浏览器查看：127.0.0.1:8080，下图表示tomcat搭建成功：

访问漏洞环境：（如果无法访问，重启Tomcat将自动部署漏洞war包）
http://127.0.0.1:8080/struts2-showcase/integration/saveGangster.action

验证漏洞环境
i.输入表达式

ii.Submit之后可看到运算被后台执行：

3.模拟RCE（远程代码执行）（确保Tomcat打开）

Centos开启httpd、iptables、关闭防火墙、设置虚拟机NAT地址和端口。详见：
http://blog.csdn.net/microsoft2014/article/details/57413491
http://linux.it.net.cn/CentOS/fast/2015/0110/11567.html

确认Centos的IP：

Kali访问Centos，执行OGNL语句：

访问：http://192.168.152.136:8080/struts2-showcase/integration/saveGangster.action

Submit后：

4.POC使用

声明文件上传：

```
%{(#szgx='multipart/form-data')
```

注入OGNL代码,通过ognl表达式静态调用获取ognl.OgnlContext的DEFAULT_MEMBER_ACCESS属性，并将获取地结果覆盖_memberAccess属性，绕过SecurityMem

```
(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.
```

判断服务器系统，调用cmd或bash：

```
(#cmd='echo dota').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.e
```

四、其他

1.复现过程中出现的问题及解决办法

Tomcat安装的时候，一开始安装我装的事7.0.8x版本，在浏览器上进不了tomcat，后来使用低版本的，成功解决这个问题。

关闭、重置Centos防火墙的时候在终端下输入命令可能会出现一些问题，这些问题一般是因为没有安装一些软件如：iptables、httpd等，解决方法已在上述说明。

模拟远端登录的时候，一定要注意攻击机输入地IP为Centos服务器地址+端口号。

上一篇：PHP安全新闻早八点-高级持续渗透... 下一篇：分享一个二进制文件上传技巧
1. 1 条追加内容
追加 于 2017年12月29日 00:41

复现getshell的视频

复现视频.zip(1.835 MB) 下载附件

---

1. 0 条回复
   - 动动手指，沙发就是你的了！

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