登录

S2-048 漏洞调试及分析

cryin / 2017-07-10 13:42:00 / 浏览数 7234 技术文章 技术文章 顶(0) 踩(0)

漏洞公告

首先看Struts2 官方给出的公告信息可得知:

Apache Struts 2.3.x版本中启用了Struts 2 Struts 1 plugin 可能导致任意代码执行漏洞

关于Struts 1 plugin:

“The Struts 1 plugin allows you to use existing Struts 1 Actions and ActionForms in Struts 2 applications.

This plugin provides a generic Struts 2 Action class to wrap an existing Struts 1 Action,org.apache.struts2.s1.Struts1Action.”

以上内容可参考Struts 1 Plugin，简单的说就是org.apache.struts2.s1.Struts1Action 类为一个Wrapper类，可以将Struts1时代的Action封装成为Struts2中的Action，以便让其可以继续在struts2应用中工作。

漏洞DEMO分析

网上已经有几篇分析很棒的文章可以参考，通过几篇分析文章可以了解到官方提供的demo程序Showcase中的Struts1 Integration就存在该漏洞，这里以struts-2.3.24-all.zip中的demo为例，详细看下代码：

SaveGangster.Action的实现类为Struts1Action，而在Struts1Action的 execute 方法中，会调用对应的Action 的 execute 方法，如下：

```
public String execute() throws Exception {
       ......
       ......
       Action action = null;

       try {
           //■■Action■■■this.className■SaveGangsterAction
           action = (Action)this.objectFactory.buildBean(this.className, (Map)null);
       } catch (Exception var12) {
           throw new StrutsException("Unable to create the legacy Struts Action", var12, actionConfig);
       }

       Struts1Factory strutsFactory = new Struts1Factory(Dispatcher.getInstance().getConfigurationManager().getConfiguration()
       ActionMapping mapping = strutsFactory.createActionMapping(actionConfig);
       HttpServletRequest request = ServletActionContext.getRequest();
       HttpServletResponse response = ServletActionContext.getResponse();
       //■■SaveGangsterAction■execute■■
       ActionForward forward = action.execute(mapping, this.actionForm, request, response);
       //■■request■ActionMessage
       ActionMessages messages = (ActionMessages)request.getAttribute("org.apache.struts.action.ACTION_MESSAGE");
       //■■ActionMessage■■■null■■■■■■■■
       if(messages != null) {
           Iterator i = messages.get();

           label36:
           while(true) {
               while(true) {
                   if(!i.hasNext()) {
                       break label36;
                   }

                   ActionMessage msg = (ActionMessage)i.next();
                   if(msg.getValues() != null && msg.getValues().length > 0) {
                       this.addActionMessage(this.getText(msg.getKey(), Arrays.asList(msg.getValues())));
                   } else {
                       //■■msg■values■null■key■Gangster ${1+3} added successfully■■■■■getText■■
                       this.addActionMessage(this.getText(msg.getKey()));
                   }
               }
           }
       }
       ......
```

通过(Action)this.objectFactory.buildBean(this.className, (Map)null);获取当前action，这里className为

```
<param name="className">org.apache.struts2.showcase.integration.SaveGangsterAction</param>
```

而该demo中SaveGangsterAction类继承了Action并重写了execute方法：

```
public class SaveGangsterAction extends Action {
   @Override
   public ActionForward execute(ActionMapping mapping, ActionForm form, HttpServletRequest request, HttpServletResponse respon

       // Some code to save the gangster to the db as necessary
       GangsterForm gform = (GangsterForm) form;
       ActionMessages messages = new ActionMessages();
       messages.add("msg", new ActionMessage("Gangster " + gform.getName() + " added successfully"));
       addMessages(request, messages);

       return mapping.findForward("success");
   }
}
```

这里同时将gforn.getName()放到了ActionMessage结构中，并添加到request，属性名为org.apache.struts.action.ACTION_MESSAGE。动态调试可以知道这里name的

```
${1+3}
```

继续往下看代码的执行流程。在调用SaveGangsterAction的execute方法后，接着检查了request中ActionMessage是否为空，不为空则对ActionMessage进行处理并回显

```
this.addActionMessage(this.getText(msg.getKey()));
```

getText函数的存在是因为Struts2要走向世界，帮助用户解决前端国际化问题。它会根据不同的Locale（本例中为zh_CN）去对应的资源文件里面获取相关文字信息并展现。

继续跟进，最后到了LocalizedTextUtil类的findText方法，这个方法分析过Struts2漏洞的都熟悉，如今年的S2-045。

```
public static String findText(Class aClass, String aTextName, Locale locale, String defaultMessage, Object[] args) {
       ValueStack valueStack = ActionContext.getContext().getValueStack();
       return findText(aClass, aTextName, locale, defaultMessage, args, valueStack);
   }
```

这里aTextName、defaultMessage均为 “Gangster ${1+3} added successfully”

查看LocalizedTextUtil.findText函数的介绍：

```
“If a message is found, it will also be interpolated. Anything within ${...} will be treated as an OGNL expression and evaluat
```

message中在${...}中的任何值都将被视为OGNL表达式被解析执行，从而导致RCE。如图

关于POC

这个漏洞并不具有通用性，且利用方式和之前的漏洞几无差别。在源代码审计的时候或许可以根据具体参数构造poc验证。可参考jas502n提供的测试POC

安全建议

S2-048漏洞原因是将用户可控的值添加到ActionMessage并在客户前端展示，导致其进入getText函数，最后message被当作ognl表达式执行。

所以开发者通过使用resource keys替代将原始消息直接传递给ActionMessage。 不要使用如下的方式

```
messages.add("msg", new ActionMessage("Gangster " + gform.getName() + " was added"));
```

参考

[1] http://bobao.360.cn/learning/detail/4078.html [2] https://github.com/jas502n/st2-048 [3] http://xxlegend.com/2017/07/08/S2-048%20%E5%8A%A8%E6%80%81%E5%88%86%E6%9E%90/ [4] http://blog.topsec.com.cn/ad_lab/strutss2-048%E8%BF%9C%E7%A8%8B%E5%91%BD%E4%BB%A4%E6%89%A7%E8%A1%8C%E6%BC%8F%E6%B4%9E%E5%

上一篇：Spring MVC Autobi... 下一篇：Iphone如何上deep web

1. 7 条回复


xxlegend 2017-07-11 04:06:21

不错

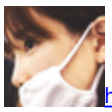
0 回复Ta


cryin 2017-07-11 05:27:24

引用第1楼xxlegend于2017-07-11 12:06发表的 ：
不错 [url=https://xianzhi.aliyun.com/forum/job.php?action=topost&tid=1844&pid=3144][/url]

炒个冷饭，基本上看着你的文章分析思路来的~

0 回复Ta


hades 2017-07-11 05:54:16

这是要比手速了么~哈哈

0 回复Ta


合肥滨湖虎子 2017-07-11 09:17:23

不错哦，重在学习安全分析的过程

0 回复Ta


 2017-07-11 13:46:28

讲真，我是真不愿看代码，哈哈。- 。- 感谢分享

0 回复Ta


cryin 2017-07-12 06:25:51

引用第5楼于2017-07-11 21:46发表的 ：
讲真，我是真不愿看代码，哈哈。- 。- 感谢分享 [url=https://xianzhi.aliyun.com/forum/job.php?action=topost&tid=1844&pid=3155][/url]

贴图体验太差，调试的图都没上。只放了一张最后结果的图～

0 回复Ta


中原 2017-07-12 09:14:45

不错，学习学习！

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