# Apache Struts2 Freemarker标签远程执行漏洞分析和复现(S2-053)

合肥滨湖虎子 / 2017-09-08 08:37:00 / 浏览数 5067 安全技术 漏洞分析 顶(0) 踩(0)

---

Author：虎子@中新网安

2017年9月7日，Struts官方发布一个中危的安全漏洞，该漏洞编号为:S2-053,在一定条件下，当开发人员在Freemarker标签中使用错误的构造时，可能会导致远程代码执行

漏洞编号

CVE-2017-12611

漏洞名称

Freemarker标签远程代码执行漏洞

漏洞评级

中危

影响范围

Struts 2.0.1 - 2.3.33
Struts 2.5 - 2.5.10

漏洞复现

idea创建默认struts2项目

执行poc

```
http://localhost:8081/zxsoft?strutsS=%25%7B%23_memberAccess%3D@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS%2C@java.lang.Runtime@get
```

代码执行成功后弹出记事本程序。

漏洞分析

当在Freemarker标签中使用表达式文本或强制表达式时，使用以下请求值可能会导致远程代码执行

```
<@s.hidden
name="strutsS" value=strutsS/>
<@s.hidden name="strutsS"
value="${strutsS}" />
```

这两种情况下，值属性都使用可写属性，都会受到Freemarker表达式影响

再将默认的execute方法执行的结果集通过DefaultActionInvocation中的createResult方法传递到ftl模板里

然后接着取出了payload

然后payload 进入ValueStack 中的map值栈，并且位于值栈的栈顶

最终FreeMarker模板使用assign指令调用struts.translateVariables方法去执行keyValue的栈顶元素

修复建议

升级Apache Struts到version 2.5.13


上一篇：ThinkerPHP后台存在远程任... 下一篇：COM Object hijack...

1. 0 条回复
   - 动动手指，沙发就是你的了！

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