

预警编号：YJ-2017018

---

**恒安嘉新**

**关于 Struts(S2-049)拒绝服务漏洞**

**安全预警通告**



**恒安嘉新（北京）科技股份有限公司**

**2017年07月11日**

## 1 漏洞描述

2017年7月11日,Apache Struts发布最新的Struts2漏洞公告-编号S2-049。该漏洞公告中说明:在一定条件下该漏洞可造成拒绝服务漏洞。该漏洞危害等级为“中危”。由于该框架是应用广泛,故恒安嘉新第一时间发布预警公告。

## 2 影响范围

Struts2.5 - 2.5.10.1

## 3 漏洞原理

Struts2 是 Apache 软件基金会负责维护的一个基于 MVC 设计模式的 Web 应用框架开源项目。

当使用 Spring Security, 并且认证成功时, 开发人员在 struts 框架中使用 SpringAOP (如: 采用 Spring Security 做权限控制), 则可能导致拒绝服务。

具体细节如下:

AOP 概念 :AOP( Aspect Oriented Programming ), 即面向切面编程。AOP 技术是利用一种称为“横切”的技术, 剖解开封装的对象内部, 并将那些影响了多个类的公共行为封装到一个可重用模块, 并将其命名为“Aspect”, 即切面。所谓“切面”, 简单说就是那些与业务无关, 却为业务模块所共同调用的逻辑或责任封装起来, 便于减少系统的重复代码, 降低模块之间的耦合度, 并有利于未来的可操作性和可维护性。

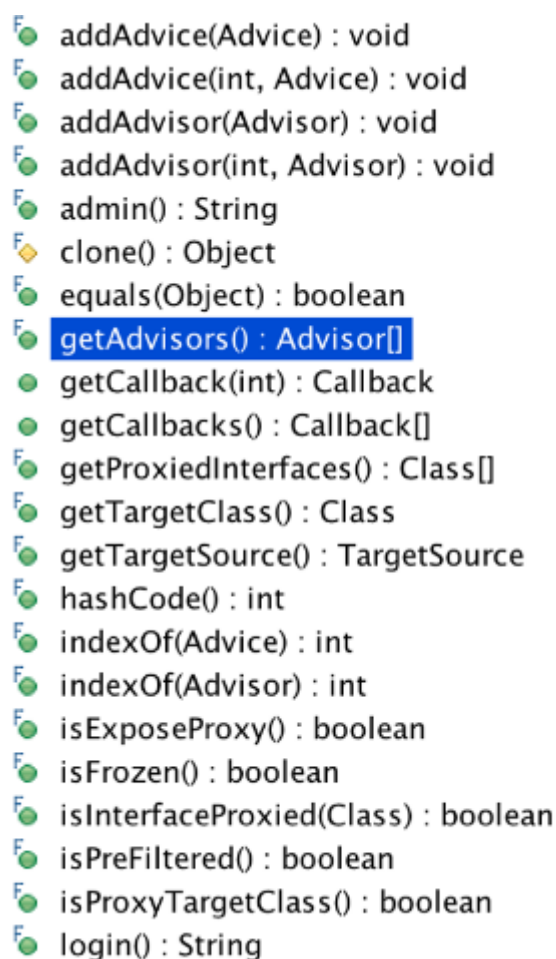
Spring 在使用 AOP 的时候存在两种代理方式：

1)如果被代理的类是接口的话则使用jdk 自带的动态代理来实现。

2)当需要代理的类不是代理接口的时候 Spring 会切换为使用 CGLIB 代理。

spring security 在使用 CGLIB 在创建 Proxy 的时候会注册。org.springframework.aop.framework.Advised 接口实现以及属性到动态生成的代理类里面。

如下图（ Spring Security 使用 aop cglib 动态增加生成的 ）：



```
addAdvice(Advice) : void
addAdvice(int, Advice) : void
addAdvisor(Advisor) : void
addAdvisor(int, Advisor) : void
admin() : String
clone() : Object
equals(Object) : boolean
getAdvisors() : Advisor[]
getCallback(int) : Callback
getCallbacks() : Callback[]
getProxiedInterfaces() : Class[]
getTargetClass() : Class
getTargetSource() : TargetSource
hashCode() : int
indexOf(Advice) : int
indexOf(Advisor) : int
isExposeProxy() : boolean
isFrozen() : boolean
isInterfaceProxied(Class) : boolean
isPreFiltered() : boolean
isProxyTargetClass() : boolean
login() : String
```

图 1 Spring Security 使用 aop cglib 动态生成图

但 Struts2 调用 Spring security AOP 代理生成的 Action ，经过 ParametersInterceptor 拦截器的时候可以设置被代理的 Action 的属性。从而导致被代理类里面某些动态设置的属性值被篡改，产生拒绝服务。可控属性如下图：

```
{ "advisors": [{"advice": {"accessDecisionManager": {"allowIfAllAbstainDecisions": false, "decisionVoters": [{"rejectPublicInvocations": false, "runAsManager": {}, "secureObjectClass": "interface org.sopalliance.inti"}, {"allConfigAttributes": null}], "validateConfigAttributes": true, "order": 2147483647, "perinstance": true, "exposeProxy": false, "frozen": false, "preFiltered": true, "proxiedInterfaces": [{"proxyTargetClass": true,
```

图 2 可控属性

## 4 修复建议

目前官方已发布补丁，用户可升级至 Struts2 2.5.12 版本。