河南省教育信息安全监测中心

Spring 远程代码执行漏洞

预警

河南省教育信息安全监测中心
Henan Provincial Education Information Security Monitoring Center

2022 年 3 月 30 日

Spring 远程代码执行漏洞预警

事件描述

Spring 是一款目前主流的 Java EE 轻量级开源框架，它提供了一系列底层容器和基础设施并可以和大量常用的开源框架无缝集成。

近日，河南省教育信息安全监测中心监测到 Spring 框架存在远程代码执行漏洞，远程攻击者可利用该漏洞在目标 Spring 系统中执行任意代码，该漏洞影响范围为全版本的 Spring 框架，前置条件为 JDK 版本为 9 以上。

影响范围

Spring 全版本（且 JDK 版本>=9）

漏洞编号

暂无

安全建议

目前，Spring 官方无官方补丁，建议采用以下两个临时方案进行防护，并及时关注官方补丁发布情况，按官方补丁修复漏洞。

1. WAF 防护

在 WAF 等网络防护设备上，根据实际部署业务的流量情况，实现对“class.*”“Class.*”“*.class.*”“*.Class.*”等字符串的规则过滤，并在部署过滤规则后，对业务运行情况进行测试，避免产生额外影响。

2. 临时修复措施

需同时按以下两个步骤进行漏洞的临时修复:

1.在应用中全局搜索@InitBinder 注解，看看方法体内是否调用 dataBinder.setDisallowedFields 方法，如果发现此代码片段的引入，则在原来的黑名单中，添加{"class.*","Class. *","*. class.*", "*.Class.*"}。 (注:如果此代码片段使用较多,需要每个地方都追加)

2. 在应用系统的项目包下新建以下全局类，并保证这个类被 Spring 加载到(推荐在 Controller 所在的包中添加).完成类添加后，需对项目进行重新编译打包和功能验证测试。并重新发布项目。

```
import org.springframework.core.annotation.Order;
import org.springframework.web.bind.WebDataBinder;
import org.springframework.web.bind.annotation.ControllerAdvice;
import org.springframework.web.bind.annotation.InitBinder;
@ControllerAdvice
@Order(10000)
public class GlobalControllerAdvice{
   @InitBinder
   public void setAllowedFields(webdataBinder dataBinder){
   String[]abd=new
string[]{"class.*","Class.*","*.class.*","*.Class.*"};
   dataBinder.setDisallowedFields(abd);
   }}
```

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893、0371-67765016

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052