

「漏洞通告」

Spring Framework 远程代码执行漏洞

安全风险通告

漏洞描述

Spring Framework 是一个开源应用框架，旨在降低应用程序开发的复杂度。它是轻量级、松散耦合的。它具有分层体系结构，允许用户选择组件，同时还为 J2EE 应用程序开发提供了一个有凝聚力的框架。

近期监测到 Spring 官方发布安全公告，披露了一个 Spring 框架可在 JDK>=9 版本下实现远程代码执行的漏洞(CVE-2022-22965)。该漏洞是由于 Spring Framework 未对传输的数据进行有效的验证，攻击者可利用该漏洞在未授权的情况下，构造恶意数据进行远程代码执行攻击，最终获取服务器最高权限。

漏洞编号

CVE-2022-22965

漏洞等级

高危

影响版本

Spring Framework 5.3.X < 5.3.18

Spring Framework 5.2.X < 5.2.20

注：其他小版本未更新均受影响


```
✓ java -version
java version "1.8.0_271"
Java(TM) SE Runtime Environment (build 1.8.0_271-b09)
Java HotSpot(TM) 64-Bit Server VM (build 25.271-b09, mixed mode)
```

2. 排查 Spring 框架使用情况

检查项目是否使用 Spring 基础框架，未使用则不受影响。可通过排查项目是否使用 spring-beans 核心依赖进行检查。

3. 排查项目部署方式

经过前两步排查后，排查项目是否使用 Tomcat 进行部署，目前利用主要针对 Tomcat 中间件，但其他中间件不排除后续被利用的可能。

4. 排查项目代码

项目中 Web 接口未使用 JavaBean 对象作为参数则不受此漏洞影响。

四、漏洞缓解措施

1、在应用中全局搜索 @InitBinder 注解，方法体中若调用 `dataBinder.setDisallowedFields`，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、若未发现，可通过 @ControllerAdvice 进行全局拦截，通过 `WebDataBinder` 中 `setDisallowedFields` 方法添加黑名单。参考代码：

```
JAVA

import org.springframework.web.bind.WebDataBinder;
import org.springframework.web.bind.annotation.ControllerAdvice;
import org.springframework.web.bind.annotation.InitBinder;

@ControllerAdvice
@Order(Ordered.LOWEST_PRECEDENCE)
public class BinderControllerAdvice {
    @InitBinder
    public void setAllowedFields(WebDataBinder dataBinder) {
        String[] denylist = new String[]{"class.*", "Class.*",
            "*.class.*", "*.Class.*"};
        dataBinder.setDisallowedFields(denylist);
    }
}
```