安全控制器SeerEngine-SEC是否涉及Spring MVC远程代码执行漏洞

漏洞相关 王树岭 2022-03-31 发表

漏洞相关信息

漏洞编号： 暂无
漏洞名称： Spring MVC远程代码执行漏洞
产品型号及版本： SeerEngine-SEC-E1106P03

漏洞描述

Spring MVC远程代码执行漏洞。

1. 影响版本

需同时满足以下条件

a) Jdk版本大于等于9

b) Spring MVC框架或衍生框架

2. 临时处置建议

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）需同时按以下两个步骤进行漏洞的临时修复:

a) 在应用中全局搜索@InitBinder注解，查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.*"}。

b) 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);
        }
    }
```

漏洞解决方案

不涉及漏洞