核弹级漏洞通告 | Spring RCE 0day漏洞

原创 动感超人 破冰安全实验室 2022-03-29 22:42

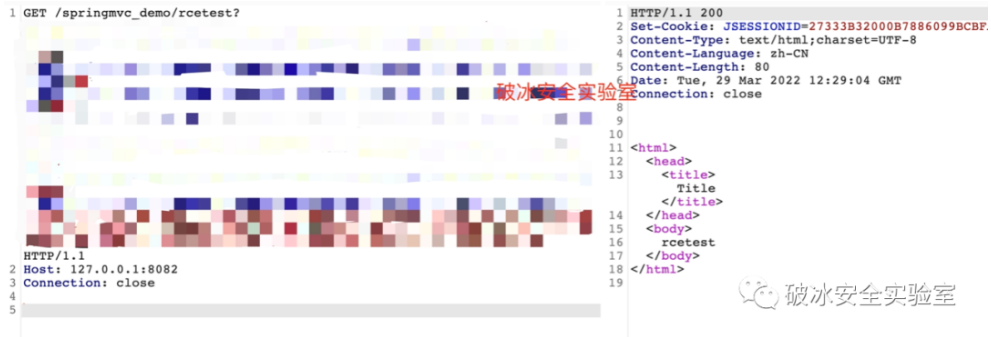
漏洞通告

PART01 漏洞简介

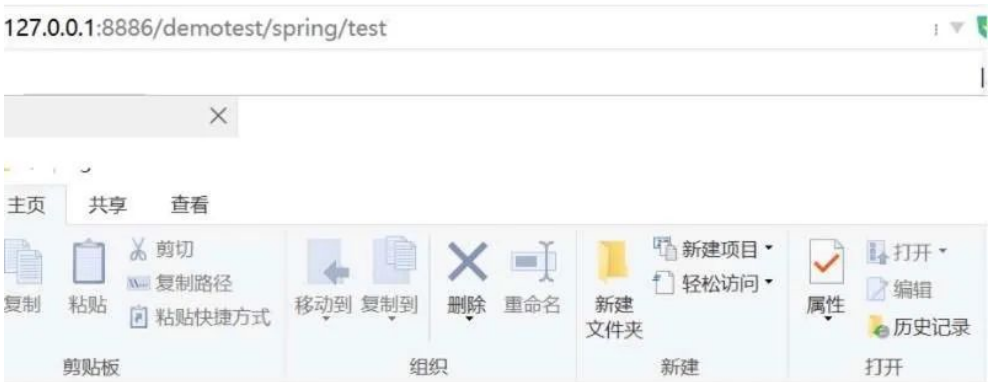
近日，破冰安全实验室监测到一则 《疑似Spring 框架RCE 0day漏洞》信息

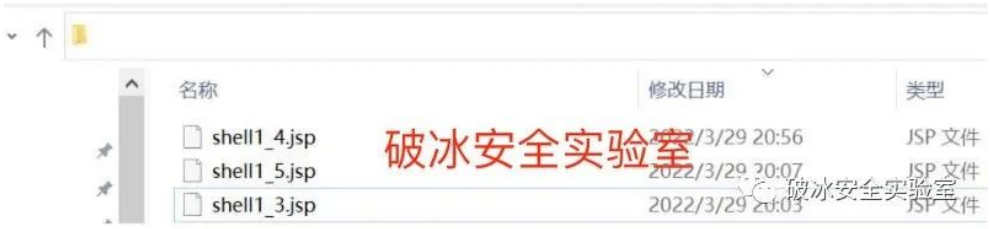
随即破冰安全实验室开展了相关漏洞研究工作，并在第一时间成功复现了此漏洞！

复现过程截图如下：



命令执行，写入文件





文件上传成功

由于该漏洞特性，可导致任意文件读取、dos攻击等危害，甚至导致业务服务器被攻陷

只要同时满足以下条件的应用系统均遭受影响：

1、使用了jdk 9及以上

2、使用tomcat部署了spring项目

3、Spring项目中web接口参数使用了复杂对象

经破冰安全实验室对该漏洞危害影响紧急分析研判后

认定该漏洞影响**范围极广**，漏洞**危害极大**

实际影响范围可能不弱于21年底的Log4j2远程命令执行漏洞

PART02 漏洞原理

Spring 是目前世界上最受欢迎的 Java EE 轻量级开源框架，是 Java 世界最为成功的框架之一。专注于简化 Java 企业级应用的开发难度、缩短开发周期。

此次Spring中存在的漏洞属于历史遗留问题，结合 jdk9 及以上新版本的特性，将会绕过 CVE-xxxx-xxxx 的补丁，再结合 tomcat 进行 spring 项目部署的实际环境中，可利用 tomcat 某些特性进行 getshell

关于 Spring RCE 0day 判断是否存在利用条件：
1、JDK 9 及以上
2、Spring 框架以及衍生的框架
spring-beans-*.jar 文件 或者 存在
CachedIntrospectionResults.class

PART03 解决方案

目前Spring官方尚未发布官方补丁，建议采用以下两个临时方案进行防护，密切关注官方补丁发布情况，按照官方补丁修复漏洞。

1 WAF 临时策略（仅供参考）

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，并在部署规则后，**对业务允许情况进行测试**，避免产生额外影响。

2 临时缓解措施（仅供参考）

1. 全局搜索 @InitBinder 注解，判断方法体内是否有dataBinder.setDisallowedFields方法，
如果有使用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.Orde
    import org.springframework.web.bind.WebData
    import org.springframework.web.bind.annotat
    import org.springframework.web.bind.annotat
    @ControllerAdvice
    @Order(10000)
    public class GlobalControllerAdvice{
        @InitBinder
        public void setAllowedFields(webdataBi
        String[]abd=new string[]{"class.*","Cl
        dataBinder.setDisallowedFields(abd);
        }
    }
```

关于破冰

破冰安全实验室是启明星辰集团CSM体系中设立的首批安全实验室，立足成都辐射西南，实验室现有红蓝对抗、漏洞挖掘、攻防竞赛、安全咨询、合规评估、应急响应6大研究方向，潜心研究同时紧跟国内外网络安全形势，专研网络安全前沿技术

紧跟国内外网络安全形势，专研网络安全前沿技术。

破冰安全实验室坚持以安全技术研究为第一生产力，赋能前场安全服务团队，为客户提供高质量渗透测试、代码审计、安全咨询、风险评估、攻防演练、CTF/AWD竞技、应急响应、安全培训、情报推送等多项个性化安全服务，推动客户网络安全建设。基于多年安全技术研究沉淀，多年大型服务项目实践积累，成功助力党政、金融、能源、运营商等多个重点行业安全保障工作。

END

喜欢此内容的人还喜欢

漏洞通告 | WPS Office 远程代码执行漏洞

破冰安全实验室