网络安全风险预警通报

2022 年第 2 期 （总第 16期）

广西大学网络信息中心 2022 年 4 月 20 日

【预警类型】 高危预警

【预警内容】

Spring 框架存在远程命令执行漏洞
漏洞风险公告

安全公告编号 CNVD-2022-23942

一、漏洞概述

Spring 框架（Framework）是一个开源的轻量级 J2EE 应用程序开发框架，提供了 IOC、AOP 及 MVC 等功能，解决了程序人员在开发中遇到的常见问题，提高了应用程序开发便捷度和软件系统构建效率。Spring 框架远程命令执行漏洞（CNVD-2022-23942）。攻击者利用该漏洞，可在

未授权的情况下远程执行命令。目前，漏洞利用细节已大范围公开，Spring 官方已发布补丁修复该漏洞。

二、漏洞详情

由于 Spring 框架存在处理流程缺陷，攻击者可在远程条件下，实现对目标主机的后门文件写入和配置修改，继而通过后门文件访问获得目标主机权限。使用 Spring 框架或衍生框架构建网站等应用，且同时使用 JDK 版本在 9 及以上版本的，易受此漏洞攻击影响。

三、漏洞影响范围

漏洞影响的产品版本包括：

版本低于 5.3.18 和 5.2.20 的 Spring 框架或其衍生框架构建的网站或应用。

三、漏洞处置建议

目前，Spring 官方已发布新版本完成漏洞修复，CNVD 建议受漏洞影响的产品（服务）厂商和信息系统运营者尽快进行自查，并及时升级至最新版本：

https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

参考链接：

https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

https://github.com/spring-projects/spring-framework/compare/v5.3.17...v5.3.18