Spring Boot 安全绕过漏洞（CVE-2023-20873）通告

■ **通告编号**	**NS-2023-00**	■ 发布日期	**2023-04-21**
■ **漏洞危害**	**攻击者利用漏洞可实现安全绕过**		
■ **TAG**	Spring Boot、身份验证绕过、CVE-2023-20873		

一. 漏洞概述

近日，绿盟科技 CERT 监测发现 Spring 官方发布安全通告，修复了一个 Spring Boot 身份验证绕过漏洞（CVE-2023-20873）。当 Spring Boot 部署到 Cloud Foundry，并存在可以处理匹配请求的代码/cloudfoundryapplication/**，且将其与/**相匹配的 catch-all request mapping 一起使用时，未经身份验证的远程攻击者可通过 Cloud Foundry 上的通配符模式匹配实现安全绕过，请受影响的用户尽快采取措施进行防护。

Spring Boot 是一种快速开发框架，它基于 Spring 框架，旨在简化 Spring 应用程序的配置和部署。

CVE-2023-20873 漏洞状态：

漏洞细节	漏洞 PoC	漏洞 EXP	在野利用
未公开	未公开	未公开	暂不存在

参考链接：

https://spring.io/security/cve-2023-20873

二. 影响范围

受影响范围

- 3.0.0 <= Spring Boot <= 3.0.5
- 2.7.0 <= Spring Boot <= 2.7.10
- 不受支持的旧版本

不受影响范围

- Spring Boot >= 3.0.6
- Spring Boot >= 2.7.11

三. 漏洞检测

在 pom.xml 的 version 标签中查看当前使用的 Spring Boot 版本号:

```
<parent>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-parent</artifactId>
    <version>2.7.5</version>
    <relativePath/> <!-- lookup parent from repository -->
</parent>
```

若 Spring Boot 版本号在受影响范围之内，则可能存在安全风险。

四. 漏洞防护

4.1 官方升级

目前官方已发布安全版本修复该漏洞，建议受影响的用户尽快升级版本进行防护，参考链接如下：

https://github.com/spring-projects/spring-boot/tags

4.2 临时防护措施

通过在配置文件中添加以下代码，以禁用 Cloud Foundry 执行器：

```
management.cloudfoundry.enabled=false
```

声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。

绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。