

Spring Framework 身份验证绕过 漏洞（CVE-2023-20860）通告

■ 通告编号 NS-2023-0015

■ 发布日期 2023-03-22

■ 漏洞危害 攻击者利用漏洞可实现身份验证绕过

■ TAG Spring Framework、身份验证绕过、CVE-2023-20860



一. 漏洞概述

近日，绿盟科技 CERT 监测到 Spring 官方发布安全通告，修复了一个 Spring Framework 身份验证绕过漏洞（CVE-2023-20860）。当 Spring Security 配置中用作""模式时，会导致 Spring Security 和 Spring MVC 之间的 mvcRequestMatcher 模式不匹配。未经身份验证的远程攻击者通过构造特制请求，最终可实现身份验证绕过访问后台信息。

Spring Framework 是一个开源的 JavaEE 应用程序框架，它提供了一种轻量级的、非侵入性的方式来构建基于 Java 的企业应用程序。

参考链接：

<https://spring.io/security/cve-2023-20860>

二. 影响范围

受影响范围

- 6.0.0 <= Spring Framework <= 6.0.6
- 5.3.0 <= Spring Framework <= 5.3.25

注意：Spring Framework 5.3 之前的版本不受影响

不受影响范围

- Spring Framework >= 6.0.7
- Spring Framework >= 5.3.26

三. 漏洞检测

3.1 版本检测

相关用户可通过版本检测的方式判断当前应用是否存在风险。

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

```
<dependency>
  <groupId>org.springframework</groupId>
  <artifactId>spring-webmvc</artifactId>
  <version>4.1.4.RELEASE</version>
</dependency>
```

若 Spring Framework 版本在受影响范围内, 则可能存在安全风险。

四. 漏洞防护

4.1 官方升级

目前官方已在最新版本中修复了该漏洞, 请受影响的用户尽快升级版本进行防护, 最新版本下载链接如下:

<https://github.com/spring-projects/spring-framework/releases/tag/v6.0.7>

<https://github.com/spring-projects/spring-framework/releases/tag/v5.3.26>

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。