Apache Shiro 身份认证绕过漏洞（CVE-2023-22602）通告

■ **通告编号**	**NS-2023-00**	■ 发布日期	**2023-01-17**
■ **漏洞危害**	**攻击者利用此漏洞，可实现身份验证绕过。**		
■ **TAG**	Apache Shiro、权限绕过、CVE-2023-22602		

一. 漏洞概述

近日，绿盟科技 CERT 监测发现 Apache 官方修复了一个身份认证绕过漏洞。当在 2.6+ 版本的 Spring Boot 中使用 Apache Shiro，且 Shiro 与 Spring Boot 使用不同的路径匹配模式时，无需身份验证的攻击者可以用此漏洞构造特制的 HTTP 请求绕过身份验证访问后台功能，请相关用户采取措施进行防护。

Apache Shiro 是一个功能强大且易于使用的 Java 安全框架，功能包括身份验证、授权、加密和会话管理。使用 Shiro 的 API，可以轻松地、快速地保护任何应用程序，范围从小型的移动应用程序到大型的 Web 和企业应用程序。

参考链接：

https://lists.apache.org/thread/dzj0k2smpzzgj6g666hrbrgsrlf9yhkl

二. 影响范围

受影响版本

- Apache Shiro < v1.11.0

不受影响版本

- Apache Shiro >= v1.11.0

三. 漏洞检测

3.1 人工检测

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。

①在 config\pom.xml 的 version 标签中查看当前使用的 shiro 版本号:

```
<!-- shiro start -->
<dependency>
    <groupId>org.apache.shiro</groupId>
    <artifactId>shiro-core</artifactId>
    <version>1.2.5</version>
</dependency>
<dependency>
    <groupId>org.apache.shiro</groupId>
    <artifactId>shiro-ehcache</artifactId>
    <version>1.2.5</version>
</dependency>
<dependency>
    <groupId>net.sf.ehcache</groupId>
    <artifactId>ehcache-core</artifactId>
    <version>2.4.8</version>
</dependency>
<dependency>
    <groupId>org.apache.shiro</groupId>
    <artifactId>shiro-spring</artifactId>
    <version>1.2.5</version>
</dependency>
<dependency>
    <groupId>org.apache.shiro</groupId>
    <artifactId>shiro-web</artifactId>
    <version>1.2.5</version>
</dependency>
<!-- end shiro -->
```

②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>
```

综上，若 shiro 版本在受影响范围内且 Spring Boot 版本号为 2.6+，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此漏洞，建议受影响的用户及时升级防护：https://shiro.apache.org/download.html

4.2 临时防护措施

若用户无法正常升级，可将 Spring Boot 的配置值设置为以下内容：

```
spring.mvc.pathmatch.matching-strategy = ant_path_matcher
```

声明