Apache Shiro 权限绕过
漏洞通告

2021 年 9 月 28 日

目录

一、 漏洞概要

漏洞名称	Apache Shiro 权限绕过漏洞（CVE-2021-41303）
影响组件	Apache Shiro
影响范围	Apache Shiro < 1.8.0
漏洞类型	绕过登录验证
利用条件	1、用户认证：不需要用户认证 2、前置条件：需要配合 Spring 3、触发方式：远程
综合评价	<综合评定利用难度>：一般。 <综合评定威胁等级>：中危，能造成登录绕过。

二、 漏洞分析

2.1 组件介绍

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。内置了可以连接大量安全数据源（又名目录）的 Realm，如 LDAP、关系数据库（JDBC）、类似 INI 的文本配置资源以及属性文件等。

2.2 漏洞描述

2021 年 9 月 17 日，深信服安全团队监测到一则 Apache Shiro 组件存在权限绕过漏洞的信息，漏洞编号：CVE-2021-41303，漏洞危害：中危。

该漏洞是由于 Apache Shiro 与 Spring 结合使用时存在绕过问题，攻击者可利用该漏洞在未授权的情况下，使用精心构造的 HTTP 请求绕过登录验证，最终造成服务器敏感性信息泄露。

三、 影响范围

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。可能受漏洞影响的资产分布于世界各地，主要分布在中国、美国、日本等国家，国内主要集中在广东、北京、上海等地

目前受影响的 Apache Shiro 版本：

Apache Shiro < 1.8.0

四、 解决方案

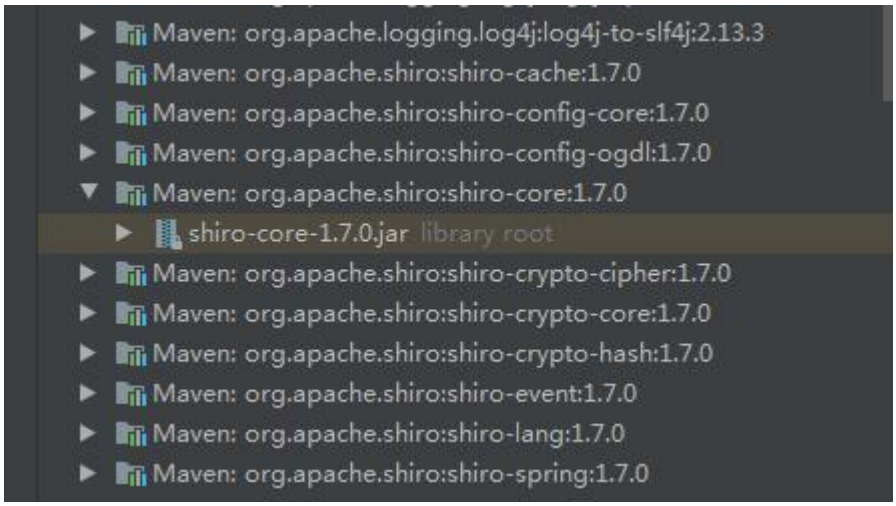
4.1、 官方解决方案

当前官方已发布最新版本，建议受影响的用户及时更新升级到最新版本。链接如下：

https://shiro.apache.org/download.html

4.2、 如何检测组件系统版本

方法一、在集成环境中查看：



注：示例为 0 1.7.0 版本。请以自己环境中 o shiro 版本为准

方法二、找到 shiro 的 jar 包，后面的包名中*.*.*即为版本号，如：

注：示例为 1 1.7.1 版本。请以自己环境中 shiro 版本为准