Jenkins 任意文件读取漏洞（CVE-2024-23897）通告

■ 通告编号	NS-2024-0006	■ 发布日期	2024-1-26
■ 漏洞危害	攻击者利用此漏洞，可实现任意文件读取。		
■ TAG	Jenkins、文件读取、CVE-2024-23897		

一. 漏洞概述

近日，绿盟科技 CERT 监测到 Jenkins 发布安全公告，修复了 Jenkins CLI 中的一个任意文件读取漏洞（CVE-2024-23897），由于 Jenkins 中默认启用其 CLI 命令解析器的一个功能，特定的解析器功能 expandAtFiles 可将@参数中后跟文件路径的字符替换为文件内容，导致攻击者可通过使用 Jenkins 控制器进程的默认字符编码读取读取 Jenkins 上的任意文件，并结合 Resource Root URL、Remember me cookie、存储型 XSS 或 CSRF 等在 Jenkins 控制器中实现任意代码执行。目前 PoC 已公开，请受影响的用户尽快采取措施进行防护。

Jenkins 是一款基于 Java 开发的开源项目，用于持续集成和持续交付的自动化中间件，可通过构建的 Pipeline 持续、自动地构建/测试软件项目，并监控软件开发流程，快速问题定位及处理。Jenkins 有一个内置的命令行界面（CLI），可从脚本或 shell 环境访问 Jenkins。当处理 CLI 命令时， Jenkins 使用 args4j 库解析 Jenkins 控制器上的命令参数和选项。

参考链接：

https://www.jenkins.io/security/advisory/2024-01-24/

二. 影响范围

受影响版本

- Jenkins <= 2.441
- Jenkins LTS <= 2.426.2

不受影响版本

- Jenkins >= 2.442
- Jenkins LTS >= 2.426.3

三. 漏洞防护

3.1 官方升级

目前官方已发布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，官方下载链接：https://www.jenkins.io/download

3.2 其他防护措施

若相关用户暂时无法进行升级操作，也可通过下列措施进行临时缓解：

禁用 Jenkins CLI：将 Java 系统属性 hudson.cli.CLICommand.allowAtSyntax 设置为 true

禁用 CLI 端点与 SSH 端口，可参考文档：https://github.com/jenkinsci-cert/SECURITY-3314-3315

声明