NSFOCUS

Jenkins 高危漏洞

安全预警通告

■ 预警编号	NS-2018-0021	■ 发布日期	2018-7-25
■ 危害等级	高，攻击者可利用爆出的漏洞，获取 Jenkins 服务器中存储的构建过程信息，甚至利用 Jenkins 脚本命令行功能，获取 Jenkins 服务器的控制权限。		
■ TAG	Jenkins、CVE-2018-1999001、CVE-2018-1999002、任意文件下载		

NSFOCUS

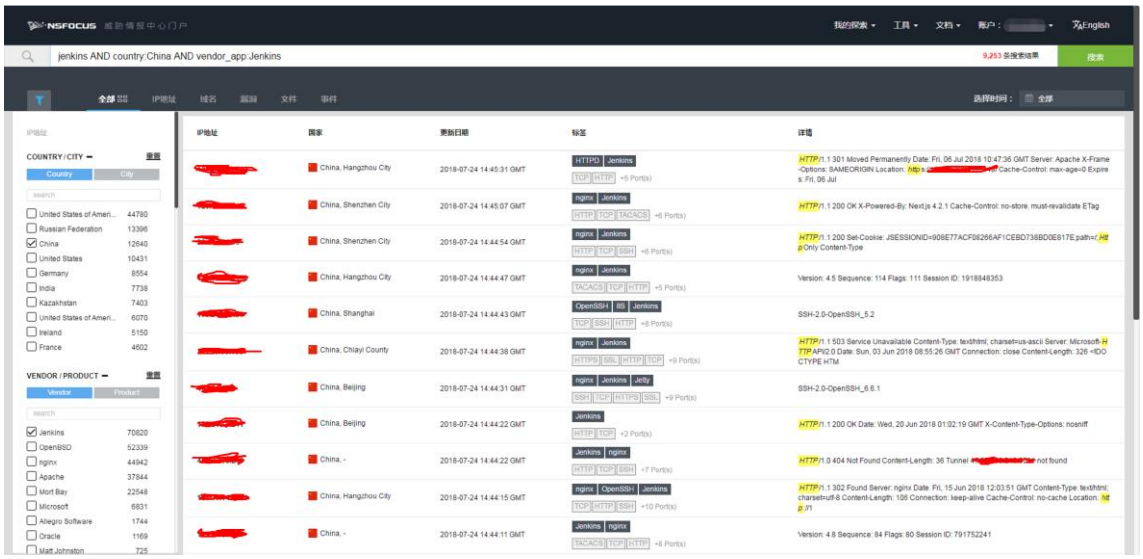
一. 漏洞概述

Jenkins 是一款基于 Java 开发的开源的、用于持续集成和持续交付的自动化中间件，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，使得开发者从繁杂的集成过程中解脱出来，专注于更为重要的业务功能实现。

北京时间 7 月 18 日，Jenkins 官方发布安全通告，修复了 7 个漏洞，其中包括一个严重漏洞（CVE-2018-1999001，Jenkins 配置文件路径改动导致管理员权限开放漏洞）和一个高危漏洞（CVE-2018-1999002，任意文件读取漏洞）。为保证 Jenkins 服务器的安全及其存储代码和构建过程数据的安全，强烈建议相关企业将 Jenkins 升级至最新版本。

漏洞编号	漏洞描述	官方漏洞评级
CVE-2018-1999001	Jenkins 配置文件路径改动导致未经身份验证的用户可越权获取管理员权限	严重
CVE-2018-1999002	任意文件读取漏洞	高危
CVE-2018-1999003	未授权用户可越权取消排队的构建	中危
CVE-2018-1999004	未授权用户可越权启动和中止代理启动	中危
CVE-2018-1999005	存储型 XSS 漏洞	中危
CVE-2018-1999006	未授权用户可越权确定何时从其 JPI 包中提取插件	中危
CVE-2018-1999007	Stapler 调试模式下的 XSS 漏洞	中危

结合绿盟威胁情报的数据，有近万个公网资产应用了 Jenkins 服务，请相关单位及时关注。



参考链接： https://jenkins.io/security/advisory/2018-07-18/

二. 影响范围

受影响的版本

- Jenkins weekly 2.132 版本及以下
- Jenkins LTS 2.121.1 版本及以下

不受影响版本

- Jenkins weekly 2.133 版本
- Jenkins LTS 2.121.2 版本

三. 解决方案

3.1 官方升级

官方在最新的版本中针对以上漏洞进行了修复，新版本下载链接如下：

Jenkins LTS 2.121.2	http://mirrors.jenkins.io/war-stable/latest/jenkins.war
Jenkins weekly 2.133	http://mirrors.jenkins.io/war/latest/jenkins.war

以 CentOS 系统下的 Jenkins 中间件升级为例，Jenkins 默认安装的文件目录应该为：/usr/lib/jenkins，按照如下过程进行升级。

1、停止 Jenkins 服务，并对 jenkins.war 进行备份；

```
service jenkins stop
cd /usr/lib/jenkins
cp jenkins.war jenkins_bak.war
```

2、删除 jenkins.war 文件；

```
rm -f jenkins.war
```

3、下载最新版 jenkins，并启动 jenkins 服务；

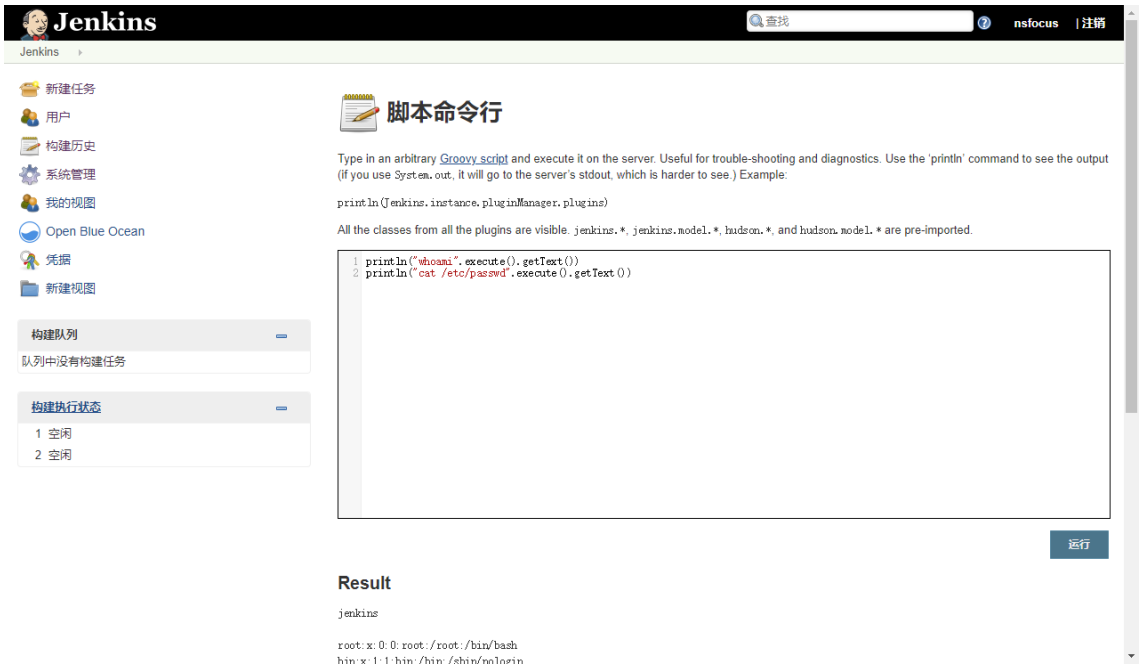
```
wget http://mirrors.jenkins.io/war-stable/latest/jenkins.war
service jenkins start
```

```
Last login: Wed Jul 25 22:51:42 2018
[root@localhost ~]# service jenkins start
Starting jenkins (via systemctl):                          [  OK  ]
[root@localhost ~]# service jenkins stop
Stopping jenkins (via systemctl):                          [  OK  ]
[root@localhost ~]# cd /usr/lib/jenkins/
[root@localhost jenkins]# ls
jenkins.war
[root@localhost jenkins]# cp jenkins.war jenkins_bak.war
[root@localhost jenkins]# ls
jenkins_bak.war  jenkins.war
[root@localhost jenkins]# rm –f jenkins.war
rm: cannot remove ‘–f’: No such file or directory
rm: remove regular file ‘jenkins.war’?
[root@localhost jenkins]# ls
jenkins_bak.war  jenkins.war
[root@localhost jenkins]# rm -f jenkins.war
[root@localhost jenkins]# wget http://mirrors.jenkins.io/war-stable/latest/jenki
ns.war
--2018-07-25 23:24:23--  http://mirrors.jenkins.io/war-stable/latest/jenkins.war
Resolving mirrors.jenkins.io (mirrors.jenkins.io)... 52.202.51.185
Connecting to mirrors.jenkins.io (mirrors.jenkins.io)|52.202.51.185|:80... conne
cted.
HTTP request sent, awaiting response... 302 Found
Location: http://mirrors.shu.edu.cn/jenkins/war-stable/2.121.2/jenkins.war [foll
owing]
--2018-07-25 23:24:25--  http://mirrors.shu.edu.cn/jenkins/war-stable/2.121.2/je
nkins.war
Resolving mirrors.shu.edu.cn (mirrors.shu.edu.cn)... 202.121.199.235
Connecting to mirrors.shu.edu.cn (mirrors.shu.edu.cn)|202.121.199.235|:80... con
nected.
HTTP request sent, awaiting response... 200 OK
```

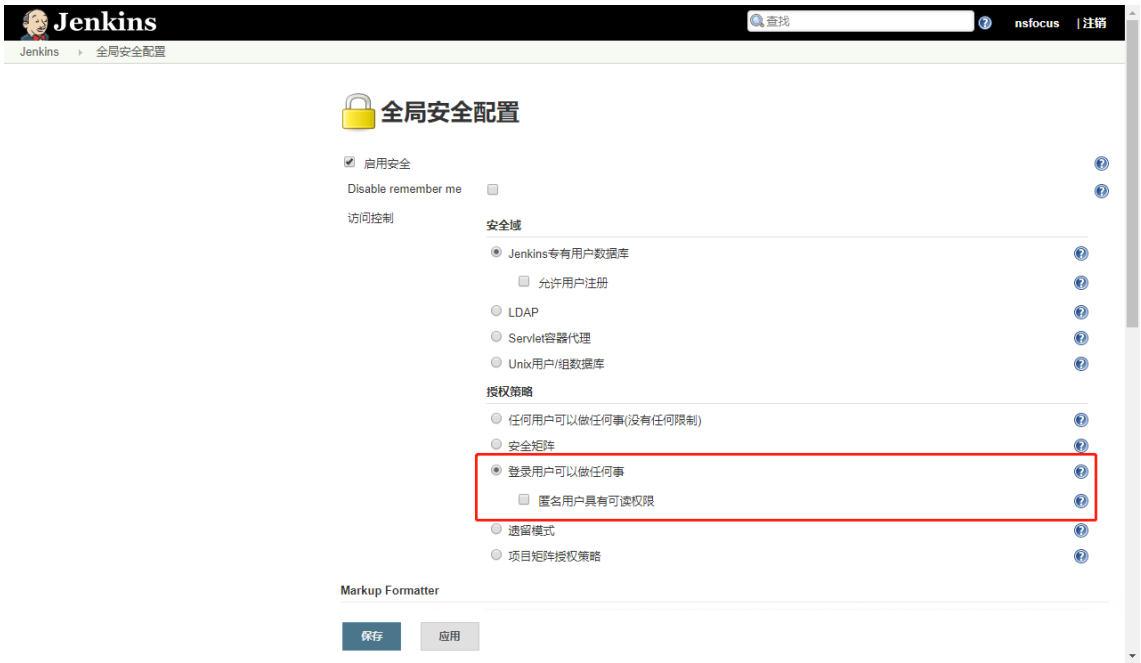
升级成功。

附录A 漏洞简述

攻击者可利用 CVE-2018-1999001 漏洞从 Jenkins 主目录下移除 config.xml 配置文件到其他目录，当 Jenkins 服务再次重启时，因加载不了 config.xml 中配置的安全域和授权策略，退回 legacy 模式，并且赋予匿名用户管理员访问权限。当攻击者获取 Jenkins 权限后，可查看构建历史数据，甚至可下载工作区的代码，导致核心代码泄露；攻击者在进入管理页面后，可通过“系统管理”下的“脚本命令行”功能，执行用于管理或故障探测或诊断的任意脚本命令，对 Jenkins 系统服务器产生比较严重的影响和危害。



CVE-2018-1999002 漏洞，可使得攻击者在 Jenkins 开启匿名用户访问权限的情况下，通过构造恶意的 HTTP 请求（在 Accept-Language 头部构造读取任意文件 payload）发往 Jenkins Web 服务端，读取 Jenkins 用户权限下的任意文件。然而，默认安装的 Jenkins 配置中的匿名用户是没有可读权限，且对于安装在 Linux 环境下的 Jenkins 利用难度较大。



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。

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。

绿盟科技官方微博二维码

绿盟科技官方微信二维码