# JumpServer 远程代码执行漏洞
# 安全通告

2021 年 1 月 19 日

# 目录

# 一、 漏洞概要

| | |
|---|---|
| 漏洞名称 | JumpServer 远程代码执行漏洞 |
| 威胁等级 | 高危 |
| 影响范围 | JumpServer < v2.6.2<br>JumpServer < v2.5.4<br>JumpServer < v2.4.5<br>JumpServer = v1.5.9 |
| 安全版本 | Fasterxml >= 2.10.x |
| 漏洞类型 | 远程执行代码 |
| 利用难度 | 一般 |

# 二、 漏洞分析

## 2.1 组件介绍

Jumpserver 是全球首款完全开源、符合 4A 规范（包含认证 Authentication、授权 Authorization、账号 Accounting 和审计 Auditing）的运维安全审计系统，Jumpserver 通过软件订阅服务或者软硬件一体机的方式，向企业级用户交付多云环境下更好用的堡垒机。

与传统堡垒机相比，Jumpserver 采用了分布式架构设计，支持多云环境并可灵活扩展。资产管理方面，Jumpserver 无并发和资产数量限制，支持水平扩容。Jumpserver 采用了业界领先的容器化部署方式，并且提供体验极佳的 WebTerminal。Jumpserver 还可实现基于 Web 的文件传输，并且支持用户将运维审计录像保存在云端。

## 2.2 漏洞描述

2021 年 1 月 15 日，深信服安全团队监测到 JumpServer 官方发布了一则漏洞安全通告，通告披露了 JumpServer 组件存在远程代码执行漏洞，漏洞等级：高危。该漏洞由于未对 JumpServer 某些接口做授权限制，攻击者可利用该漏洞在未授权情况下，构造恶意数据获取服务器敏感信息，最终可造成服务器敏感性信息泄露，或者通过执行相关 API 操作执行任意代码，最终可控制其中所有机器。

# 三、 影响范围

## 3.1. 受影响版本

JumpServer < v2.6.2

JumpServer < v2.5.4

JumpServer < v2.4.5

JumpServer = v1.5.9

# 四、 解决方案

## 4.1、官方解决方案

当前官方已发布受影响版本的对应补丁，建议受影响的用户及时更新官方的安全补丁。链接如下：

https://github.com/jumpserver/jumpserver/blob/master/README.md

## 4.2、临时解决方案

该临时修复建议存在一定风险，建议用户可根据业务系统特性审慎选择采用 临时修复方案：

**修改 Nginx 配置文件屏蔽漏洞以下接口：**

/api/v1/authentication/connection-token/

/api/v1/users/connection-token/

**Nginx 配置文件位置：**

# 社区老版本

/etc/nginx/conf.d/jumpserver.conf

# 企业老版本

jumpserver-release/nginx/http_server.conf

# 新版本在

jumpserver-release/compose/config_static/http_server.conf

**修改 Nginx 配置文件实例：**

```
### 保证在/api 之前和/之前
location /api/v1/authentication/connection-token/
{ return 403; }
location /api/v1/users/connection-token/ { 5 return
403; }
### 新增以上这些
location /api/ {
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header Host $host;
proxy_set_header X-Forwarded-For
$proxy_add_x_forwarded_for;
proxy_pass http://core:8080;
}
```