河南省教育信息安全监测中心
关于 JumpServer 远程代码执行漏洞
的安全风险预警

河南省教育信息安全监测中心
Henan Provincial Education Information Security Monitoring Center

2024 年 4 月 3 日

关于 JumpServer 远程代码执行漏洞的安全风险预警

漏洞说明

JumpServer 是使用广泛的开源堡垒机，使用 GNU GPL v2.0 开源协议，是符合 4A 规范的运维安全审计系统。

CVE-2024-29201：由于 JumpServer 中的 Ansible 模块未进行完整的输入验证，具有低权限账户的攻击者可以绕过输入验证机制在 Celery 容器中执行任意代码，并从主机中窃取敏感信息或操纵数据库。

CVE-2024-29202：经过身份验证的攻击者可以通过构建恶意 playbook 模板，利用 Ansible 中的 Jinja2 模板引擎在 Celery 容器中执行任意代码，并从主机中窃取敏感信息或操纵数据库。

漏洞编号

CVE-2024-29201

CVE-2024-29202

影响版本

- v3.0.0 <= JumpServer <= v3.10.6

安全建议

1.官方升级

目前官方已在最新版本中修复了上述漏洞，请受影响的用户尽快升级版本进行防护，下载链接：https://github.com/jumpserver/jumpserver/releases

2.临时防护措施

若相关用户暂时无法进行升级操作，也可通过关闭作业中心功能进行临时缓解：

使用管理员账户登录 JumpServer 堡垒机后台，依次选择“系统设置”→“功能设置”→“任务中心”，点击按钮关闭作业中心功能。

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893、0371-67765016

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052