

点击搜索



文章速查

Cordys 1Panel
JumpServer MaxKB
DataEase SQLBot
MeterSphere
CloudExplorer
安全通知

分类目录

Cordys

Zabbix

1Panel

JumpServer

新闻

活动

观点

案例研究

操作教程

安全通知

MaxKB

说明 | 关于JumpServer CVE-2023-48193漏洞披露的相关说明

发布于 2023年12月08日 JumpServer JumpServer/安全通知 安全通知

2023年11月28日，JumpServer开源项目组收到了编号为CVE-2023-48193的漏洞报告（<https://nvd.nist.gov/vuln/detail/CVE-2023-48193>）。报告显示，JumpServer开源堡垒机存在允许远程攻击者绕过命令过滤功能执行任意代码的漏洞。JumpServer开源项目组在第一时间关注到了该漏洞所披露的相关信息，并进行了测试和验证。

经过分析和验证，CVE-2023-48193漏洞报告主要围绕JumpServer开源堡垒机的命令过滤功能展开。命令过滤功能使用的前提是在堡垒机软件上输入命令，堡垒机针对这些命令进行匹配并执行相应的阻断、审核等动作。而关于其他形式的命令过滤场景，例如通过各类脚本语言编写的未编译程序、编程语言编译的程序等实现同等命令效果的场景，在堡垒机中无法进行相应的管控操作。这也是由堡垒机的产品设计特性所决定的。

JumpServer开源堡垒机的产品定位是一款以“无插件、无侵入式”方式部署的运维安全审计平台。JumpServer不会在用户所纳管的Linux服务器中安装任何Agent代理插件，在用户操作过程中也不会实时读取系统运行的进程并进行实时管控。因为在系统管理与业务应用运行的过程中，安装此类型的监控和管理Agent代理插件通常是不被允许的，目的是避免出现潜在的安全风险。

针对CVE-2023-48193漏洞本身，其影响的是拥有对应资产登录权限的堡垒机用户，这类用户有机会去执行危险的操作。而在企业内部，防止这些危险操作的发生可以通过JumpServer开源堡垒机的其他功能来实现。通过授权和复核场景进行控制，用户可以有效防范相关的安全隐患。

JumpServer开源项目组总结了三种可以有效控制用户异常操作的方法，能够有效提升堡垒机日常操作的安全性，提供给大家作为参考，具体如下：

通过资产授权功能，更加精确地控制用户拥有的资产和账号权限。例如，通过“仅授权非Root权限级别的账号”等权限控制手段，将用户拥有的账号权限限制在管理员可控范围之内，防止用户做出影响系统运行安全的操作；

通过会话分享功能，进入多人协作模式。例如，在进行核心系统和应用的维护变更时，采用双人复核协作的方式来进行责任分担，提高系统运维的安全性和可靠性；

通过资产登录控制功能，限制用户登录资产的时间、地点，以及是否需要管理员进行二次复核。例如，用户在登录安全性较高的资产时，必须由管理员进行审核并通过后才被允许登录。

感谢广大用户对JumpServer开源项目的关注和支持。

JumpServer开源项目组
2023年12月8日

[上一篇](#)

[社区分享 | 简米Ping++基于MeterSphere开展异地测试...](#)

[下一篇](#)

[新增模板中心和系统设置模块，支持飞书平台对接，DataEas..](#)

DataEase

[新闻](#)

[仪表板展示](#)

[案例研究](#)

[操作教程](#)

[学习笔记](#)

[模板学堂](#)

[安全通知](#)

SQLBot

MeterSphere

[新闻](#)

[活动](#)

[观点](#)

[案例研究](#)

[操作教程](#)

[安全通知](#)

CloudExplorer

[新闻](#)

[观点](#)

[案例研究](#)

[市场研究](#)

[媒体洞察](#)

[操作教程](#)

[公司新闻](#)

精品推荐

[JumpServer开源堡垒机与腾讯云TDSQL数据...](#)

[飞致云开源社区月度动态报告（2026年6月）](#)

[喜报 | Cordys开源AI CRM系统全网累计下...](#)

[操作教程 | 在WorkBuddy中使用...](#)

[“JumpServer+MaxKB”合AI智能运维审计方案](#)

[修复安全漏洞并增强查询组件功能，DataEa...](#)

[飞致云与宏时数据联合发布Zabbix信创一体机](#)

[案例研究 | 河南医药健康技师学院“药院小智”...](#)

[里程碑 | MaxKB开源企业级智能体平台v2.10...](#)

[1Panel AI网关：企业级AI流量调度中枢](#)

FIT2CLOUD 飞致云

我们秉持“软件用起来才有价值，才有改进的机会”的核心价值观，向中国数字化团队交付被广泛验证、可信赖的通用工具软件。

快速浏览

- > 关于我们
- > 开源社区
- > 如何购买

联系我们

- > support@fit2cloud.com
- > 400-052-0755

关注我们



浙ICP备14038283号

© 2014-2024 杭州飞致云信息科技有限公司 版权所有