

【附POC】1Panel远程命令注入漏洞复现 (CVE-2025-54424)

漏洞介绍

1Panel v2 是一款现代化的开源服务器运维管理面板，主打极简、轻量、高扩展性。相比于 v1，1Panel v2 引入了主从节点架构，支持集中式管理多台服务器，通过统一的 Web UI 实现批量部署、统一监控与任务调度。此外，v2 架构更注重模块化和插件生态，支持 Docker 快速部署常用服务，提升运维效率。适用于中小企业、开发者以及个人用户构建私有云、搭建服务环境或统一管理多台主机。

1Panel (一个用于 Linux 服务器的 Web 管理界面及 MCP Server) 在 2.0.5 及更早版本中，核心组件 (Core) 和代理组件 (Agent) 之间的 HTTPS 通信未执行完整的证书验证，攻击者可借此绕过认证，访问敏感接口。这些接口包括命令执行和高权限操作，最终可能导致远程代码执行 (RCE)



漏洞版本

- 1Panel是v2版本（只有v2版本存在主从节点）
- 1Panel版本 <= v2.0.5

漏洞利用

使用CVE-2025-54424.py漏洞利用Python脚本进行漏洞利用，使用方法如下：

```
(CommonPython) a1battr0ss@MacBookAir ~ % python CVE-2025-54424.py -h
usage: CVE-2025-54424.py [-h] -u URL

1Panel RCE Exploit Tool

options:
  -h, --help            show this help message and exit
  -u URL, --url URL    Single target for exploitation. Example: 127.0.0.1:9999
```

使用 `python CVE-2025-54424.py -u IP:PORT` 成功获取到目标root权限：

漏洞修复

修复需要将版本升级

- **1Panel** v2.0.6及以上版本已经修复该漏洞