

資通訊設備盤點

日期：2025-01-10

目錄

內

容

- 資通訊設備盤點
- 大陸廠牌盤點
- 資通訊設備風險控管

資通訊設備盤點

資通訊設備盤點注意事項

- 盤點範圍：
 - 可透過連接網路提供服務的設備
 - 學校採購與公務使用之設備
- 盤點方法：
 - 準備財產清單，逐一核對設備
 - 準備單位IP清冊，逐一核對IP使用情形
- 輔助工具：
 - nmap、Shodan、Censys

輔助工具：Shodan

The screenshot displays the Shodan search engine interface. At the top, there is a navigation bar with links for Shodan, Maps, Images, Monitor, Developer, and More... The main search bar contains the IP address 'ip:140.112.41.0/24' and a search icon. The results are categorized into 'TOTAL RESULTS' (112), 'TOP PORTS', 'TOP PRODUCTS', and 'TOP OPERATING SYSTEMS'. A 'Product Spotlight' banner is also visible.

TOTAL RESULTS
112

TOP PORTS

Port	Count
3389	14
443	12
22	10
80	10
137	8

[More...](#)

TOP PRODUCTS

Product	Count
Remote Desktop Protocol	14
nginx	14
OpenSSH	11
Apache httpd	6
Apple remote desktop vnc	3

[More...](#)

TOP OPERATING SYSTEMS

OS	Count
Linux	6
Windows 11 (version 22H2) (build 10.0.22621)	5
Mac OS X	4
Windows (build 10.0.19041)	4
Synology Router Manager (SRM) 1.2.5-8227	2

[More...](#)

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

140.112.41.252 2024-12-30T19:07:18.819469
xdn41o252.ee.ntu.edu.tw
[Ministry of Education Computer Center](#)
Taiwan, Taipei

NTP
protocolversion: 3
stratum: 0
leap: 3
precision: -18
rootdelay: 0.0
rootdisp: 1.00001525879
refid: 0
reftime: 0.0
poll: 4

140.112.41.53 2024-12-22T09:17:42.891541
xdn41o53.ee.ntu.edu.tw
[Ministry of Education Computer Center](#)
Taiwan, Taipei

Program	Version	Protocol	Port
portmapper	4	tcp	111
portmapper	3	tcp	111
portmapper	2	tcp	111
portmapper	4	udp	111
portmapper	3	udp	111
portmapper	2	udp	111

301 Moved Permanently [↗](#) 2024-12-30T13:44:41.456677
140.112.41.126
chopin.ee.ntu.edu.tw
[Ministry of Education Computer Center](#)
Taiwan, Taipei

HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Mon, 30 Dec 2024 13:44:40 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive
Location: https://140.112.41.126/
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff

輔助工具：Censys

Limited Time Beta Program Access: Censys Internet Intelligence Platform is here! [Try it first! →](#)

censys

Results [Try CensysGPT Beta](#) [Report](#) [Docs](#) [Subscriptions](#)

Host Filters

Labels:

- 41 remote-access
- 23 network-administration
- 7 file-sharing
- 6 login-page
- 6 network.device.vpn
- More

Autonomous System:

- 60 NTU-TW National Taiwan University

Location:

- 60 Taiwan

Service Filters

Service Names:

- 47 HTTP
- 37 SSH
- 21 UNKNOWN
- 14 RDP
- 8 NETBIOS
- More

Ports:

- 22 22
- 15 3389
- 13 443
- 12 80
- 9 123
- More

Hosts
Results: 60 Time: 0.01s

- 140.112.41.218 (mil.ee.ntu.edu.tw)**
NTU-TW National Taiwan University (17716) Taiwan, Taiwan
authentication remote-access
>_ 22/SSH 80/HTTP 88/KERBEROS 137/NETBIOS 443/HTTP
5900/VNC 22000/UNKNOWN
- 140.112.41.52 (gestalt.ee.ntu.edu.tw)**
Linux NTU-TW National Taiwan University (17716) Taiwan, Taiwan
remote-access vue.js network-administration
>_ 22/SSH 80/HTTP 111/PORTMAP 111/PORTMAP 123/NTP
137/NETBIOS 389/LDAP 443/HTTP 636/LDAP 873/UNKNOWN
3260/ISCSI 3265/UNKNOWN 5000/HTTP 5001/HTTP
- 140.112.41.230 (telstar.ee.ntu.edu.tw)**
Microsoft Windows NTU-TW National Taiwan University (17716) Taiwan, Taiwan
remote-access network-administration
>_ 222/SSH 3389/RDP 17500/UNKNOWN 56435/UNKNOWN 56535/UNKNOWN
56635/UNKNOWN
- 140.112.41.19 (xdn41o19.ee.ntu.edu.tw)**
NTU-TW National Taiwan University (17716) Taiwan, Taiwan
80/HTTP 443/HTTP
- 140.112.41.219 (xdn41o219.ee.ntu.edu.tw)**
NTU-TW National Taiwan University (17716) Taiwan, Taiwan
authentication remote-access

輔助工具：nmap

C:\Users
Starting
Nmap sca
Host is
Not show
PORT
113/tcp

Nmap sca
Host is
Not show
PORT
80/tcp
443/tcp
501/tcp
8443/tcp

```
output - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明
method="table" conf="3"/></port>
<port protocol="tcp" portid="6281"><state state="open" reason="syn-ack" reason_ttl="60"/></port>
</ports>
<times srtt="728" rttvar="507" to="100000"/>
</host>
<host starttime="1735632420" endtime="1735635002"><status state="up" reason="echo-reply" reason_ttl="60"/>
<address addr="140.112.41.53" addrtype="ipv4"/>
<hostnames>
<hostname name="xdn41o53.ee.ntu.edu.tw" type="PTR"/>
</hostnames>
<ports><extraports state="closed" count="65530">
<extrareasons reason="reset" count="65530" proto="tcp" ports="1-21,23-110,112-134,136-138,140-444,446-65535"/>
</extraports>
<port protocol="tcp" portid="22"><state state="open" reason="syn-ack" reason_ttl="60"/><service name="ssh"
method="table" conf="3"/></port>
<port protocol="tcp" portid="111"><state state="open" reason="syn-ack" reason_ttl="60"/><service name="rpcbind"
method="table" conf="3"/></port>
<port protocol="tcp" portid="135"><state state="filtered" reason="no-response" reason_ttl="0"/><service name="msrpc"
method="table" conf="3"/></port>
<port protocol="tcp" portid="139"><state state="filtered" reason="no-response" reason_ttl="0"/><service name="netbios-
ssn" method="table" conf="3"/></port>
<port protocol="tcp" portid="445"><state state="filtered" reason="no-response" reason_ttl="0"/><service
name="microsoft-ds" method="table" conf="3"/></port>
</ports>
<times srtt="546" rttvar="535" to="100000"/>
</host>
<host starttime="1735632420" endtime="1735634953"><status state="up" reason="echo-reply" reason_ttl="60"/>
<address addr="140.112.41.54" addrtype="ipv4"/>
<hostnames>
<hostname name="xdn41o54.ee.ntu.edu.tw" type="PTR"/>
</hostnames>
<ports><extraports state="closed" count="65530">
<extrareasons reason="reset" count="65530" proto="tcp" ports="1-21,23-110,112-134,136-138,140-444,446-65535"/>
</extraports>
<port protocol="tcp" portid="22"><state state="open" reason="syn-ack" reason_ttl="60"/><service name="ssh"
method="table" conf="3"/></port>
<port protocol="tcp" portid="111"><state state="open" reason="syn-ack" reason_ttl="60"/><service name="rpcbind"
method="table" conf="3"/></port>
<port protocol="tcp" portid="135"><state state="filtered" reason="no-response" reason_ttl="0"/><service name="msrpc"
method="table" conf="3"/></port>
<port protocol="tcp" portid="139"><state state="filtered" reason="no-response" reason_ttl="0"/><service name="netbios-
ssn" method="table" conf="3"/></port>
<port protocol="tcp" portid="445"><state state="filtered" reason="no-response" reason_ttl="0"/><service
name="microsoft-ds" method="table" conf="3"/></port>
</ports>
```

問

資通訊設備盤點

基本資料

填報單位 

資訊網路組 

資通訊設備名稱 

資通訊設備名稱，ex.計中1樓事務機

資通訊設備IP 

IP寫法是140.112.1.1

資通訊設備廠牌型號 

範例:NTU牌 E316-9

資通訊設備存放建築物 

 搜尋

是否修改預設密碼 

是 

使用者/管理者 

設備類別 

網路印表機/多功能事務機 

資通訊設備網址/DOMAIN 

沒有的話請填無

資通訊設備版本號/作業系統版本號 

如無則填無

資通訊設備存放位置 

是否使用遠端維護 

是 

備註 

資通訊設備盤點欄位

資通訊設備名稱

- 請填寫可以識別此資通訊設備的名稱或者電腦名稱。
- NTU牌事務機
- **DESKTOP-5A1234S**

設備類別(可連網之設備)

- 請選擇資通訊設備的類別，如果超過這些類別請聯繫諮詢專線(65013、65012)。
- 伺服器及測試機請填資通訊系統。
- 網路印表機/多功能事務機
- 使用者電腦
- 智慧家電
- **DNS Server**
- 網路攝影機
- 自設門禁設備
- 環控系統
- 自設無線網路基地台(AP)/路由器
- 連網電子看板
- 能源管理系統(EMS)
- 網路磁碟NAS
- 智慧電表

資通訊設備盤點欄位

是否修改預設密碼

- 使用手冊、操作手冊
- **Google**搜尋設備型號



是否使用遠端維護

- 查詢設備防火牆設定
- 遠端維護的連線如下範例:
 - Microsoft RDP遠端桌面(3389)
 - TeamViewer(5938)
 - telnet(23)、SSH(22)
 - 設備管理介面(80、443、8443)

大陸廠牌盤點

大陸廠牌資通訊產品盤點

基本資料

填報單位 

資訊網路組

資通訊產品名稱 

如有英文名稱，以括號加註於後

廠牌名稱(中文及英文) 

如有英文名稱，以括號加註於後

產品型號或版本 

如無則填N/A

分類 

軟體

軟體及服務細項分類 

作業系統

產品是否具供不特定人士直接收視或收聽之功能 

是

委外調查

是否屬委外案廠商(含分包商)使用之產品 

不是

大陸廠牌資通訊產品盤點

汰換調查

仍未汰換原因(請敘明原因)🔗

範例:無使用需求，但未達保存年限。行政院已核定同意使用。

汰換前配套措施或相應作為🔗

停用(封存) ▼

汰換產品之經費缺口(無則填0)🔗

0

預訂汰換時間🔗

2024/12/31 🗓

汰換產品之經費估算(無則填0)🔗

0

提報調查

111年已提報且經本署核定屬盤點範圍🔗

是 ▼

111年未提報但本次提報原因🔗

如經雙資安長同意，數位部核定(請填數位部核定文號)

財產調查

資通訊產品購置年份🔗

109年以前 ▼

資通訊產品財產編號🔗

請填臺大產編，如無則填N/A

資通訊設備風險控管

網路IP分享器管理介面暴露在公開網路上

IoT掃描檢測服務

◆ 網路IP分享器113年 10 月份至 113 年 11月份：重複出現共122筆，資料如下 (第1頁)

IP	區網	單位	產品
140.112.2.1	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-AC1500UHP
140.112.2.2	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-AX88U
140.112.2.3	台大區網中心	國立臺灣大學	ASUS Wireless Router R8000P
140.112.2.4	台大區網中心	國立臺灣大學	ASUS Wireless Router GT-AX11000
140.112.2.5	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-AX1800HP
140.112.2.6	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-AX3000
140.112.2.7	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-AC58U
140.112.2.8	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-AX1800S
140.112.2.9	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-AC52
140.112.2.10	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-AX57 Go
140.112.2.11	台大區網中心	國立臺灣大學	ASUS Wireless Router GT-AX11000 Pro
140.112.2.12	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-AX1800S
140.112.2.13	台大區網中心	國立臺灣大學	Linksys WRT45G modified dropbear sshd
140.112.2.14	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-AC51U
140.112.2.15	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-AC1200
140.112.2.16	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-N12HP B1
140.112.2.17	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-AX1800S
140.112.2.18	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-AX88U Pro
140.112.2.19	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-AC1200 V2
140.112.2.20	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-AC68U
140.112.2.21	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-AC53
140.112.2.22	台大區網中心	國立臺灣大學	ASUS Wireless Router ZenWiFi AX Mini
140.112.2.23	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-N18U
140.112.2.24	台大區網中心	國立臺灣大學	ASUS Wireless Router TUF-AX5400
140.112.2.25	台大區網中心	國立臺灣大學	ASUS Wireless Router RT-AC66U B1



FTP匿名登入

```

1104
1105 Nmap scan report for [redacted].tw (140.
1106 Host is up (0.0060s latency).
1107
1108 PORT      STATE      SERVICE
1109 21/tcp    open      ftp
1110 | ftp-anon: Anonymous FTP login allowed (FTP code 230)
1111 | Can't get directory listing: TIMEOUT
1112 2121/tcp  filtered  ccproxy-ftp
1113
1114 Nmap scan report for [redacted].tw (140.
1115 Host is up (0.0060s latency).
1116
1117 PORT      STATE      SERVICE
1118 21/tcp    open      ftp
1119 2121/tcp  filtered  ccproxy-ftp
1120
1121 Nmap scan report for [redacted].tw (140.
1122 Host is up (0.0056s latency).
1123
1124 PORT      STATE      SERVICE
1125 21/tcp    open      ftp
1126 | ftp-anon: Anonymous FTP login allowed (FTP code 230)
1127 |-FWX.FWX.FWX 1 |hen |en | 80669 Dec 04 2023 | [redacted] | [redacted]
1128 |-FWX.FWX.FWX 1 |hen |en | 223062 Jan 16 2017 | [redacted] | [redacted]
1129 |-FWX.FWX.FWX 1 |hen |en | 91217 Jan 16 2017 | [redacted] | [redacted]
1130 |-FWX.FWX.FWX 1 |hen |en | 101098 Jan 16 2017 | [redacted] | [redacted]
1131 |-FWX.FWX.FWX 1 |hen |en | 343550 Jan 18 2017 | [redacted] | [redacted]
1132 |-FWX.FWX.FWX 1 |hen |en | 97465 Mar 02 2017 | [redacted] | [redacted]
1133 |-FWX.FWX.FWX 1 |hen |en | 27312 Sep 25 2017 | [redacted] | [redacted]
1134 |-FWX.FWX.FWX 1 |hen |en | 694574 Aug 01 2018 | [redacted] | [redacted]
1135 |-FWX.FWX.FWX 1 |hen |en | 838724 Jun 18 2019 | [redacted] | [redacted]
1136 |-FWX.FWX.FWX 1 |hen |en | 233018 Apr 16 2019 | [redacted] | [redacted]
1137 |-FWX.FWX.FWX 1 |hen |en | 2661860 May 19 2020 | [redacted] | [redacted]
1138 |-FWX.FWX.FWX 1 |hen |en | 1253540 Jun 16 2020 | [redacted] | [redacted]
1139 |-FWX.FWX.FWX 1 |hen |en | 6428198 Feb 18 2020 | [redacted] | [redacted]
1140 |-FWX.FWX.FWX 1 |hen |en | 1034757 Dec 12 2022 | [redacted] | [redacted]
1141 |-FWX.FWX.FWX 1 |hen |en | 802013 Aug 02 2022 | [redacted] | [redacted]
1142 |-FWX.FWX.FWX 1 |hen |en | 634047 Oct 26 2023 | [redacted] | [redacted]
1143 |-FWX.FWX.FWX 1 |hen |en | 803073 Mar 22 2023 | [redacted] | [redacted]
1144 |-FWX.FWX.FWX 1 |hen |en | 4542447 Jun 13 2023 | [redacted] | [redacted]
1145 |-FWX.FWX.FWX 1 |hen |en | 138878 Mar 27 10:52 | [redacted] | [redacted]
1146 |-FWX.FWX.FWX 1 |hen |en | 1296043 May 12 2023 | [redacted] | [redacted]
1147 |-FWX.FWX.FWX 1 |hen |en | 2553921 Apr 16 13:35 | [redacted] | [redacted]
1148 |-FWX.FWX.FWX 1 |hen |en | 2335554 Jan 08 14:41 | [redacted] | [redacted]
1149 |-FWX.FWX.FWX 1 |hen |en | 2330949 Mar 27 13:36 | [redacted] | [redacted]
1150 |-FWX.FWX.FWX 1 |hen |en | 260993 Mar 27 13:36 | [redacted] | [redacted]
1151 |-FWX.FWX.FWX 1 |hen |en | 266752 Apr 08 18:34 | [redacted] | [redacted]
1152 |-FWX.FWX.FWX 1 |hen |en | 58411 Jun 17 11:24 | [redacted] | [redacted]
1153 |-FWX.FWX.FWX 1 |hen |en | 126464 Jun 19 15:24 | [redacted] | [redacted]
1154 |-FWX.FWX.FWX 1 |hen |en | 148992 Mar 13 11:02 | [redacted] | [redacted]
1155 |-FWX.FWX.FWX 1 |hen |en | 139264 Mar 20 11:59 | [redacted] | [redacted]
1156 |-FWX.FWX.FWX 1 |hen |en | 141312 Mar 19 15:56 | [redacted] | [redacted]
1157 |-FWX.FWX.FWX 1 |hen |en | 863838 May 12 2023 | [redacted] | [redacted]
1158 |-FWX.FWX.FWX 1 |hen |en | 21858 Nov 25 2019 | [redacted] | [redacted]
1159 |-FWX.FWX.FWX 1 |hen |en | 962408 May 12 2023 | [redacted] | [redacted]
1160 |-FWX.FWX.FWX 1 |hen |en | 1263175 May 12 2023 | [redacted] | [redacted]
1161 |-FWX.FWX.FWX 1 |hen |en | 1388005 May 12 2023 | [redacted] | [redacted]
1162 |-FWX.FWX.FWX 1 |hen |en | 982801 May 22 2023 | [redacted] | [redacted]
1163 |-FWX.FWX.FWX 1 |hen |en | 1017661 May 22 2023 | [redacted] | [redacted]
1164 |-FWX.FWX.FWX 1 |hen |en | 886863 May 12 2023 | [redacted] | [redacted]
    
```

掃描過程

```

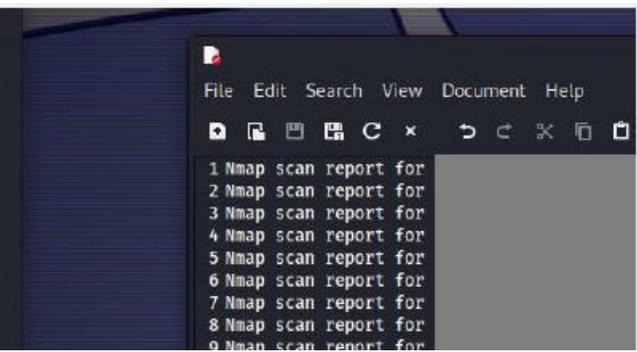
221 Operation successful
(kali@kali)~/Desktop/ftp_scan
$ ftp 140
Connected to 140.
220 FTP Utility FTP server (Version 1.00) ready.
Name (140.136.186.14:kali): anonymous
331 Password required for anonymous.
Password:
230 User anonymous logged in.
ftp> quit
221 Goodbye.

(kali@kali)~/Desktop/ftp_scan
$ ftp 140
Connected to 140.
220 Welcome to Quick 'n Easy FTP Server
Name (140.136.213.69:kali): anonym
331 Password required for anonym
Password:
230 User successfully logged in.
Remote system type is UNIX.
Using binary mode to transfer fi
ftp> quit
221 Bye

(kali@kali)~/Desktop/ftp_sc
$ ftp 163
Connected to
220 FUJI XEROX DocuPrint CP305 d
Name (163.17.181.40:kali): anonym
331 Password required for anonym
Password:
230 User anonymous logged in.
ftp> quit
221 Goodbye.

(kali@kali)~/Desktop/ftp_sc
$ ftp 140
Connected to 140.
220 FUJI XEROX DocuPrint CP305 d
Name (140.137.4.224:kali): anonym
331 Password required
Password:
230 Logged in
Remote system type is UNIX.
Using binary mode to transfer fi
ftp> quit
221 Goodbye

(kali@kali)~/Desktop/ftp_sc
$
    
```



領據/Receipt

*申請非中華民國境內居住之個人費用，本單據請依規定三日內送至會計室報帳核銷 (1120101 修正)

中華民國 112 年 [redacted] 月 [redacted] 日

茲收到 [redacted] 大學
 發給 [redacted] 校長 演講費
 代扣稅額(Tax)NT: 0
 代扣補充保費(Premium) NT: 0
 給付金額(Amount Before Tax Deducted)NT: [redacted] 0
 實領金額(Amount After Tax Deducted)NT: [redacted] 0

領款人 /Receiver	<input checked="" type="checkbox"/> [redacted] (請本人親筆以正簽名/Please sign your name here.)	國立 [redacted] 大學 (服務機關/Workplace)	093 [redacted] (聯絡電話或手機/Phone or Cell No.)
本國人 /Locals	國民身分證統一編號 <input checked="" type="checkbox"/> A> [redacted]	<input type="checkbox"/> 在本國已除戶籍請勾選 <input type="checkbox"/> 出示補充保費豁免證明	
外國人 /Foreigners	1. 統一證號 (Alien Resident Certificate ID No.)	西元出生年 BIRTH YEAR	月 MONTH
	2. 無統一證號	日 DATE	護照英文名字欄前兩碼 (FIRST TWO LETTERS GIVEN OF NAME)

新竹 [redacted] 路 [redacted] 號 [redacted] F之一

(提供之帳號須為本人帳戶，無法代為領取)請擇一填寫

未設定密碼(網路印表機)



HP Color LaserJet M653

HP Color LaserJet M653

資訊 一般 列印 耗材 故障排除 **安全性** HP Web 服務 網路

一般安全性

帳戶政策

⚠️ 存取控制

保護儲存的資料

管理遠端應用程式

憑證管理

網路服務安全性

安全性記錄

自我測試

一般安全性

設定本機管理員密碼

您可以設定管理員密碼，以防止未經授權的使用者從遠端設定裝置或在控制面板上存取為網路管理員保留的功能。此密碼也是裝置的裝置管理員存取碼。

使用者名稱

admin

舊密碼

密碼未設定。

新密碼

確認密碼

預設帳號密碼可登入(網路印表機)

Model : ECOSYS M5520cdn
Host Name : [REDACTED]46E
Location : [REDACTED]1...

Home English Auto-refresh Last Updated : 2023/04/22 12:08:30

Account Login Admin Login

User Name
Password
Login

Device Information >
Job Status >
Links

Device Status

Device	Status
Printer	Sleeping...
Scanner	Sleeping...
FAX	Ready.
Status Message	Sleeping...

Paper

Source	Size	Type	Capacity	Status
Cassette 1	A4	Plain	250	Paper Loaded
MP Tray	A5-R	Plain	50	No Paper

Toner

Color	Status
Black	85%
Cyan	32%
Magenta	35%
Yellow	24%
Waste Toner	OK

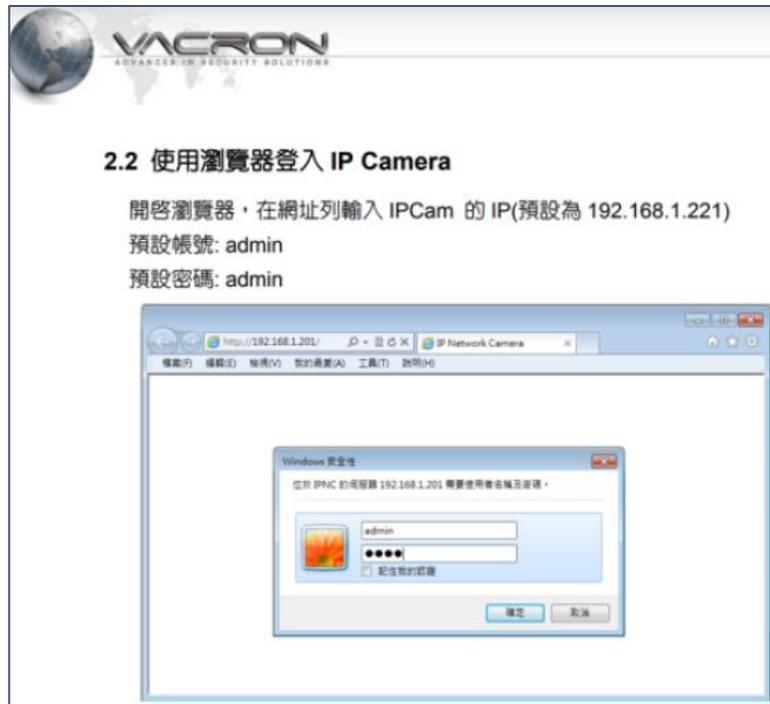
ECOSYS M5520cdn default password

全部 圖片 影片 購物 新聞 更多 工具

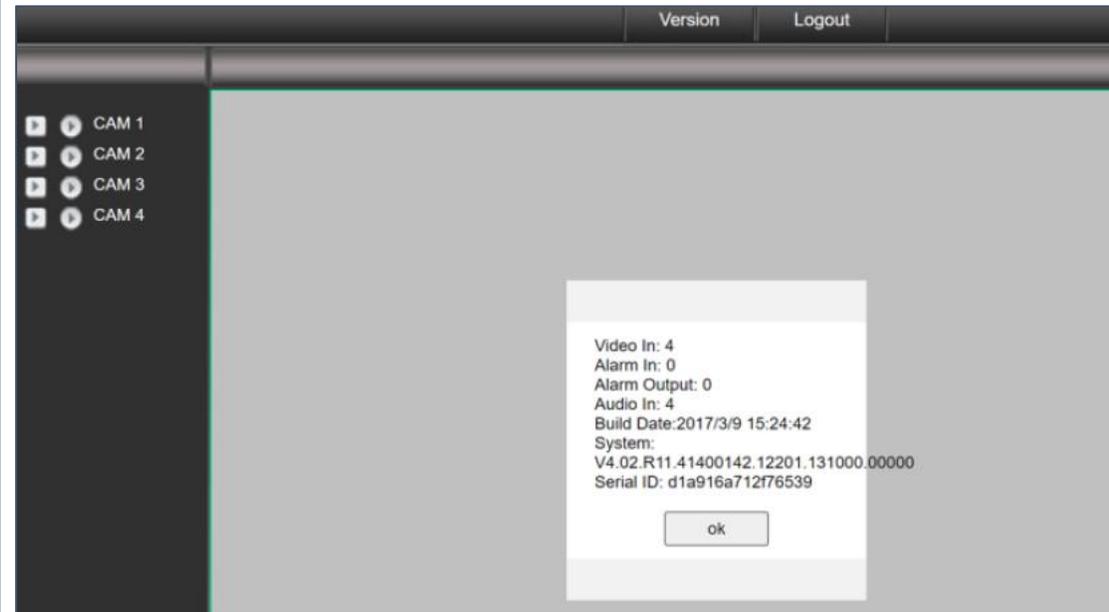
約有 446 項結果 (搜尋時間 : 0.38 秒)

The default login is **Admin** (capital A) for both the Username and PW. If the issue persists, try a different browser.

預設帳號密碼可登入(攝影機)



The image is a screenshot of a VACRON web page titled "2.2 使用瀏覽器登入 IP Camera". It provides instructions for accessing the camera via a browser. The text reads: "開啟瀏覽器，在網址列輸入 IPCam 的 IP(預設為 192.168.1.221)", "預設帳號: admin", and "預設密碼: admin". Below the text is a screenshot of a web browser window showing the IP Network Camera interface. A Windows Security dialog box is overlaid on the browser window, displaying the message: "位於 IPNC 的應用程式 192.168.1.201 需要您使用帳戶密碼。" The dialog box shows the "admin" username and a masked password field, with "確定" (OK) and "取消" (Cancel) buttons at the bottom.



The image shows the main interface of the VACRON IP camera. At the top right, there are "Version" and "Logout" buttons. On the left side, there is a vertical menu with four camera icons labeled "CAM 1", "CAM 2", "CAM 3", and "CAM 4". The main area is a large grey rectangle. In the bottom right corner of this area, there is a white box containing system information: "Video In: 4", "Alarm In: 0", "Alarm Output: 0", "Audio In: 4", "Build Date: 2017/3/9 15:24:42", "System: V4.02.R11.41400142.12201.131000.00000", and "Serial ID: d1a916a712f76539". An "ok" button is located at the bottom of this information box.

Router(路由器) CVE 弱點

D-Link 路由器未經驗證的 RCE (CVE-2019-16920)

語系: 繁體中文

CRITICAL

Nessus Plugin ID 166889

訊息

相依性

相依項目

變更日誌

概要

遠端路由器受到一個遠端程式碼執行弱點影響。

描述

遠端 D-Link 路由器受到一個遠端程式碼執行弱點影響。D-Link 產品 (如 DIR-655C、DIR-866L、DIR-652 和 DHP-1565) 中發生未經驗證的遠端程式碼執行問題。當攻擊者將任意輸入傳送至可導致一般插入的 PingTest 裝置通用閘道介面時，就會發生此問題。攻擊者若成功觸發命令插入，即可全面入侵系統。後來，還單獨發現此問題也會影響下列產品：DIR-855L、DAP-1533、DIR-862L、DIR-615、DIR-835 和 DIR-825。

請注意，Nessus 並未測試此問題，而是僅依據路由器自我報告的型式作出判斷。

解決方案

升級為受支援的裝置。

另請參閱

<https://www.seebug.org/vuldb/ssvid-98079>

<https://www.kb.cert.org/vuls/id/766427>

<https://www.fortiguard.com/zeroday/FG-VD-19-117>

Plugin 詳細資訊

嚴重性: Critical

ID: 166889

檔案名稱: d-link_router_FG-VD-19-117.nasl

版本: 1.1

類型: remote

系列: CGI abuses

發布日期: 2022/11/3

更新日期: 2022/11/3

風險資訊

CVSS v2

風險因素: Critical

基本分數: 10

媒介: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Router(路由器) CVE 弱點驗證(PoC)

```
(root@kali)-[/iot]
└─# python3 CVE-2019-16920.py 192.168.0.1 80 ping%20192.168.0.101
[*]Sending payload
[*]Exploited!
```

```
(root@kali)-[/iot]
└─# tcpdump -i eth1 -p icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
02:56:29.879792 IP 192.168.0.101 > router.dlink.com: ICMP echo request, id 19797, seq 1, length 64
02:56:29.880554 IP router.dlink.com > 192.168.0.101: ICMP echo reply, id 19797, seq 1, length 64
02:56:30.887921 IP 192.168.0.101 > router.dlink.com: ICMP echo request, id 19797, seq 2, length 64
02:56:30.888777 IP router.dlink.com > 192.168.0.101: ICMP echo reply, id 19797, seq 2, length 64
```

資通訊設備(IoT)漏洞公告

TVN (Taiwan)

iThome

blueyonder.com - if you continue to ignore
pisp#####
info#####
espr#####

Cleo | 零時差漏洞 | CVE-2024-50623 | 勒索
Yonder | Termit

遭到Cleo零時的企業超過60 體Clop揚言不 受害公司名稱

根據資安新聞網站Bleeping Computer、Security



思科 | Cisco | 收購

思科計畫收購 防禦廠商Snap 強Splunk SIE

思科在12月16日宣布
SnapAttack，以強化
陣容

- TVN (Eng)
- TVN 漏洞

全部

TVN I

TVN-2024110

TANet

COMPUTER EMERGENCY RESPONSE TEAM

即時訊息
漏洞通告
資安通報
資安文件
關於我們

台灣學術網路危機處理中心

TAIWAN >>>

安全通報

回首頁 ENGLISH

微軟安全通報 [其它安全通報]

其它安全通報

關鍵字: 查詢

第一頁 | 上一頁 | 下一頁 | 最終頁

日期	標題
2024-12-20	【漏洞預警】 Apache Struts 2存在安全漏洞(CVE-2024-53677)，請儘速確認並進行修補
2024-12-17	【漏洞預警】 中華電信 文件傳輸程式 - Reflected Cross-site Scripting to RCE
2024-12-02	【漏洞預警】 英特內 DreamMaker 之 Arbitrary File Upload through Path Traversal
2024-11-21	【漏洞預警】 WordPress外掛Really Simple Security存在安全漏洞(CVE-2024-10924)，請儘速確認並進行修補
2024-11-19	【漏洞預警】 統睿科技DVC文件保險系統存在多個重大資安漏洞

Page 1/140

<https://www.twcert.org.tw/>
<https://www.ithome.com.tw/security>
<https://cert.tanet.edu.tw/prog/index.php>

安裝新的資通訊設備建議

若無對外
公開之需求
請使用虛擬IP
(10.112.x.x)

設定非
原廠預設
之
帳號密碼

定期確認
是否有
需更新
之軟(韌)體

每年執行
盤點

若使用實體IP
確認系統設定
皆
符合安全原則

定期關注
設備是否
包含
CVE漏洞

感謝各位！