

內網印表機狂噴攻擊代碼致資源耗盡： 事件調查與防護建議

2025/05/12

黃O弘

【一、事件背景】

- 2025/04/24 清晨發現多台內網印表機遭入侵行為觸發，自動巨量列印出目錄遍歷、帳號破解等攻擊指令，初判內部設備遭惡意控制。
- 目前已知涉及印表機（均屬 172.20.XX.XX 區段）：
 - 電算中心秘書室印表機
 - 電算中心二樓大印表機
 - 電算中心一樓大印表機
 - 教務處等其他單位數台印表機

【二、資安通報】

教育機構資安通報平台

事件類型:入侵事件警訊

| | | | |
|-------|--|-------|---------------------|
| 原發布編號 | NTUSOC-102-202504-ntuasoc-20250423-164902 | 原發布時間 | 2025-04-24 08:15:13 |
| 事件類型 | 惡意程式 | 原發現時間 | 2025-04-24 00:00:23 |
| 事件主旨 | 教育部資安通告-國立中央大學[140.115.184.185]主機進行惡意程式連線(MALWARE-CNC Win.Trojan.VShell variant outbound connection attempt) | | |
| 事件描述 | 原始紀錄: MALWARE-CNC Win.Trojan.VShell variant outbound connection attempt, 入侵偵測防禦系統偵測到來源IP(140.115.184.185), 包含疑似惡意程式連線行為特徵之封包, 對目標IP(154.201.69.143)進行連線, 原始事件觸發時間: 2025-04-23 16:49:04。此事件來源 PORT(53918), 目標 PORT(8080)。 | | |
| 手法研判 | | | |
| 建議措施 | 請檢視來源IP該連線行為是否已得到合法授權。若來源IP該連線為異常行為, 可先利用掃毒軟體進行全系統掃描, 並利用ACL暫時阻擋該可疑IP。同時建議管理者進行以下檢查: a.請查看來源IP有無異常動作(如: 新增帳號、開啟不明Port、執行不明程式)。b.確認防毒軟體的病毒碼已更新為最新版本, 並進入系統安全模式下進行全系統掃描作業、系統是否已安裝相關修正檔, 或關閉不使用的應用軟體與相關通訊埠。若來源IP為DNS server、NAT主機或IP分享器等設備IP時, 表示有內部主機透過這些設備向外連線時而觸發偵測規則, 則需先請設備管理者透過事件單所附之資訊(目的地IP、時間、來源port), 來協助查找內部觸發偵測規則之主機, 再依前述建議處理措施進行作業。 | | |

【三、學務處回報】

  @ncu.edu.tw Apr 24, 2025, 10:32 AM (5 days ago)
to center108, ebr347jay, ringochiu, kcliou, center2, center38 ▼

 [Translate to Chinese \(Traditional\)](#) ×

您好
回覆如下

- (1)機器IP: 140.115.184.185
- (2)機器型號:ASUS-M900-MDR
- (3)作業系統: Windows 11 專業版 24H2
- (4)保管人: 
- (5)作何用途:學務處 
- (6)防火牆或其他防護功能:PC-Cillin
- (7)如何處理:
 - 1.封鎖攻擊ip:154.201.69.143的所有連線
 - 2.重新啟動防火牆
 - 3.執行完整掃毒，未發現惡意程式。
 - 4.已刪除被新增的使用者帳戶 `$admin01`

 敬上

【四、安全性紀錄】

1. 電算中心秘書室印表機的安全性紀錄進行溯源分析
2. 發現來源 IP 140.115.184.185 於 4/24 凌晨異常大量連線並列印
3. 列印內容為典型的滲透測試指令與目錄遍歷攻擊樣態
4. 巧合發現 140.115.184.185 為已遭入侵之學務處主機

```
outcome=success"}, {"key": 1649, "time": "2025-04-23T01:56:31.064Z", "timestamp": "133898469910640000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-23 09:56 AM (UTC+08:00))" job_name=(Microsoft Word - 文件2) user=(DESKTOP-876HTUD\\baby" source_IP=(140.115.11.105)"
outcome=success"}, {"key": 1650, "time": "2025-04-23T02:08:57.302Z", "timestamp": "133898477373020000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-23 10:08 AM (UTC+08:00))" job_name=(Microsoft Word - 附件6_國家資通安全總局與情資分享 合作備忘-01) user=(DESKTOP-5D8K0MB\\vincu57534"
source_IP=(140.115.11.157)"
outcome=success"}, {"key": 1651, "time": "2025-04-23T03:08:54.658Z", "timestamp": "133898513346580000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-23 11:08 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1652, "time": "2025-04-23T03:08:57.299Z", "timestamp": "133898513372990000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-23 11:08 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1653, "time": "2025-04-23T03:08:58.659Z", "timestamp": "133898513386590000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-23 11:08 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1654, "time": "2025-04-23T03:09:07.044Z", "timestamp": "133898513470440000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-23 11:09 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1655, "time": "2025-04-23T03:09:09.049Z", "timestamp": "133898513490490000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-23 11:09 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1656, "time": "2025-04-23T03:09:11.166Z", "timestamp": "133898513511660000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-23 11:09 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1657, "time": "2025-04-23T03:09:13.121Z", "timestamp": "133898513531210000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-23 11:09 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1658, "time": "2025-04-23T04:16:59.080Z", "timestamp": "1338985419080000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-23 12:16 PM (UTC+08:00))" job_name=(115-119年度校務發展計畫主軸五議程-會議版.pdf-01) user=(DESKTOP-5D8K0MB\\vincu57534" source_IP=(
140.115.11.157)"
outcome=success"}, {"key": 1659, "time": "2025-04-23T06:33:52.754Z", "timestamp": "133898636327540000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-23 02:33 PM (UTC+08:00))" job_name=(Microsoft Word - 20250401收農調漲後之停用先開預聞收據的部份.docx) user=(DESKTOP-876HTUD\\baby"
source_IP=(140.115.11.105)"
outcome=success"}, {"key": 1660, "time": "2025-04-23T16:59:57.266Z", "timestamp": "133899011972660000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-24 12:59 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1661, "time": "2025-04-23T16:59:59.230Z", "timestamp": "133899011992300000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-24 12:59 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1662, "time": "2025-04-23T17:00:01.234Z", "timestamp": "133899012012340000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-24 01:00 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1663, "time": "2025-04-23T17:00:03.249Z", "timestamp": "133899012032490000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-24 01:00 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1664, "time": "2025-04-23T17:00:05.247Z", "timestamp": "133899012052470000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-24 01:00 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1665, "time": "2025-04-23T17:00:07.271Z", "timestamp": "133899012072710000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-24 01:00 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1666, "time": "2025-04-23T17:00:09.261Z", "timestamp": "133899012092610000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-24 01:00 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1667, "time": "2025-04-23T17:00:12.080Z", "timestamp": "133899012120800000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-24 01:00 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1668, "time": "2025-04-23T17:00:13.268Z", "timestamp": "133899012132680000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-24 01:00 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1669, "time": "2025-04-23T17:00:15.276Z", "timestamp": "133899012152760000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-24 01:00 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1670, "time": "2025-04-23T17:00:17.268Z", "timestamp": "133899012172680000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-24 01:00 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1671, "time": "2025-04-23T17:00:19.276Z", "timestamp": "133899012192760000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-24 01:00 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
outcome=success"}, {"key": 1672, "time": "2025-04-23T17:00:21.338Z", "timestamp": "133899012213380000", "priority": 6, "firmwareVersion": "2411226_066600", "bootCycle": 176, "syslogMessage": "Print job completion, time=(2025-Apr-24 01:00 AM (UTC+08:00))" job_name=( user=(Guest" source_IP=(140.115.184.185)"
```

【五、攻擊樣本初步分析-1】

```
GET /systemController/showOrDownByUrl.do?down=&dbPath=../../../../../../../../etc/pa
Host: 172.20.11.238:9100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
Accept-Language: zh-CN,zh;q=0.9
Accept-Encoding: gzip
```

分析：

➡ GET 請求：攻擊者發送一個 HTTP 讀取指令，目標呼叫 `/systemController/showOrDownByUrl.do`，並透過參數 `dbPath=../../../../../../../../etc/passwd` 執行目錄跳脫（`../` 用於返回上層目錄），

企圖讀取 `/etc/passwd`。

➡ Host：目標伺服器為 `172.20.11.238`，使用 `9100` 埠（原本為 `DIPRINT` 列印用途，於此次被濫用作為攻擊指令傳輸通道）。

✓ 小結

攻擊者偽裝成一般正常請求，實際結合 GET 指令與目錄跳脫技巧，試圖直接存取系統敏感檔案 `/etc/passwd`，屬於典型的目錄遍歷攻擊（Directory Traversal Attack）。

【五、攻擊樣本初步分析-2】

```
GET /Audio/1/hls/../../../../Windows%5Cwin.ini/stream.mp3/ H
Host: 172.20.11.238:9100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
Accept-Language: zh-CN,zh;q=0.9
Accept-Encoding: gzip
```

分析：

➔ GET 請求：攻擊者向 `/Audio/1/hls/../../../../Windows%5Cwin.ini/stream.mp3` 發送讀取指令，企圖透過多層目錄跳脫（`%5C` 為 URL 編碼的反斜線 `\`，用於模擬 Windows 路徑結構），存取 Windows 系統設定檔 `C:\Windows\win.ini`。

✓ 小結

攻擊者利用目錄跳脫技術，嘗試讀取 Windows 系統內部設定檔 `win.ini`，驗證目錄存取控制是否鬆散，屬於**目錄遍歷攻擊（Directory Traversal Attack）**的常見探測手法。

【五、攻擊樣本初步分析-3】

```
POST /login.php HTTP/1.1
Host: 172.20.11.238:9100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
Content-Length: 50
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

username=admin&password=admin?show+webmaster+user
```

分析：

➡ **POST 請求**：攻擊者向 /login.php 發送登入表單，帳號（**username**）和密碼（**password**）都設定為 **admin**，為典型的預設弱密碼嘗試。

➡ **傳送內容**：後方夾帶 **?show+webmaster+user**，推測嘗試在登入後進行額外操作或注入指令（例如列出系統管理者帳號）。

✅ **小結**：攻擊者以 **admin:admin** 組合嘗試暴力登入（**Brute Force**），並可能試圖利用弱驗證點進行指令注入。

屬於典型的弱密碼暴力破解攻擊加橫向探索嘗試。

【五、攻擊樣本初步分析-4】

```
POST /inter/ajax.php?cmd=get_user_login_cmd HTTP/1.1
Host: 172.20.11.117:9100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
Content-Length: 85
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

{"get_user_login_cmd":{"name":"admin","password":"21232f297a57a5a743894a0e4a80
```

🔍 分析：

- POST 請求：攻擊者對 /inter/ajax.php 發送登入請求，傳送帳號 (name) 與密碼 (password) 。
- 傳送內容：admin:21232f297a57a5a743894a0e4a801fc3 (這是一組MD5雜湊值，對應明文密碼是 admin)
- 目的推測：攻擊者嘗試使用 admin/admin 預設帳密登入，屬於典型弱密碼暴力測試行為。

✅ 小結：

攻擊者試圖透過 admin/admin 這組弱密碼進行登入測試，顯示攻擊以弱點探測及暴力破解初步掃描為主，屬常見入侵前偵查行為。

【五、攻擊樣本初步分析-5】

```
POST /user.php HTTP/1.1
Host: 172.20.11.118:9100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
Content-Length: 39
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/x-www-form-urlencoded
Referer: 45ea207d7a2b68c49582d2d22adf953aads|a:2:{s:3:"num";s:193:"*/SELECT 1,
Accept-Encoding: gzip

action=login&pp123=printf(43801*42758);
```

分析：

- POST 請求：針對 /user.php 送出異常參數 pp123，試圖執行 `printf(43801*42758);`。
- 攻擊方式：利用表單傳入惡意參數，試圖觸發遠端代碼執行漏洞（RCE）或指令注入。
- 目的推測：如果伺服器端對輸入內容未做嚴格驗證，並且直接以 `eval()`、`assert()` 等方式執行參數，那麼即使單純的乘法運算也能被執行，進而證明伺服器正在解析並執行攻擊者傳入的內容，後續即可插入任意惡意指令。
- ✓ 小結：攻擊者明顯試圖以惡意參數注入觸發伺服器端執行非法運算，

屬遠端程式碼執行（RCE）預備行為，危害等級高。

【六、資安執行小組及 SNMG 通報】

center108 <center108@ncu.edu.tw> Fri, Apr 25, 3:12 PM (4 days ago)

各位資安執行與 SNMG 小組成員您好：

昨日清晨，本校部分單位發生印表機異常大量列印惡意內容的狀況。

🔥 攻擊情境如下：

攻擊者疑似入侵校內某台電腦後進行橫向移動，並透過內部網路大量發送列印命令至單位印表機，使用協定為 TCP Port 9100 (DIPRINT / RAW 模式)，導致印表機在數分鐘內自動噴出上百張惡意 payload 內容。

🔥 為避免再次發生，請各單位儘速採取以下資安防護措施：

- 1 限制來源 IP (最重要)**
 - 請啟用印表機的防火牆或存取控制清單 (ACL)，僅允許貴單位所屬內部網段 (例如資管系，140.115.80.X、140.115.82.X) 連線與列印，並封鎖其他來源
- 2 停用 DIPRINT / RAW 模式 (Port 9100)**
 - 本次攻擊即透過 DIPRINT (TCP 9100) 進行大量列印指令注入，建議一律關閉此通訊埠
 - 請改用下列較安全之列印協定：
 - ✅ LPR (Port 515)
 - ✅ IPP (Port 631)
 - 停用後，請使用者同步調整印表機設定，將通訊協定由 RAW 改為 LPR，並將 Queue Name 設為 print (小寫)；若單位導入 IPP，亦請協助切換使用。
- 3 停用「訪客列印」或「未驗證列印」等開放式功能**
- 4 更新印表機韌體**
- 5 若尚未遷入 172.20.X.X 區段，請儘速完成遷移**
 - 為強化印表機管理與存取控管，請各單位儘快將印表機遷入校內統一規劃之 172.20.X.X 區段
 - ⚠️ 本次事件雖以內網設備為主要攻擊目標，但若印表機同時暴露於對外 IP 或開放存取，將面臨更嚴重資安風險
- 6 強化印表機管理介面密碼與存取保護**
 - 請確認印表機 Web 管理介面已設定複雜密碼，避免使用出廠預設帳密 (如 admin/admin、admin/空白)
 - 密碼建議符合以下原則：
 - 至少 8-12 字元
 - 含大寫、小寫、數字、特殊符號

【七、電算中心印表機防護處置】

- 強化存取限制：
防火牆白名單限定 140.115.XX.0/24
- 封鎖攻擊通道：
停用 TCP 9100 (DIPRINT / RAW) ，僅開啟 LPR (515) 、IPP (631)
- 系統更新：
印表機進行韌體升級 (建議由廠商協助進行)
- 管理介面強化：
密碼全面更新至至少10碼，含英文大小寫、數字、特殊符號

【七、電算中心印表機防護處置 - HP】

- 強化存取限制：防火牆白名單限定 140.115.XX.0/24

HP Color LaserJet M651
NPIBEE366 172.20.11.117

資訊 一般 列印 耗材 故障排除 安全性 HP Web 服務 **網路**

設定
TCP/IP 設定
網路設定
其它設定
AirPrint
選擇語言
安全
設定
授權
安全通訊
管理通訊協定
802.1X 驗證
IPsec/防火牆
通告代理
診斷
網路統計資料
通訊協定資訊
設定頁

IPsec/防火牆政策

啟用 IPsec/防火牆

IPsec/防火牆規則

| 規則 | 啟動 | 符合準則 | | 符合動作 |
|----|-------------------------------------|------|------|------|
| | | 位址範本 | 服務範本 | 動作 |
| 1 | <input checked="" type="checkbox"/> | | | |
| 2 | <input checked="" type="checkbox"/> | | | |
| 3 | <input type="checkbox"/> | | | |
| 4 | <input type="checkbox"/> | | | |
| 5 | <input type="checkbox"/> | | | |
| 6 | <input type="checkbox"/> | | | |
| 7 | <input type="checkbox"/> | | | |
| 8 | <input type="checkbox"/> | | | |
| 9 | <input type="checkbox"/> | | | |
| 10 | <input type="checkbox"/> | | | |

預設規則 所有 IP 位址 所有服務 放棄

新增規則... 刪除規則... 進階

IPsec/防火牆政策

規則 3：指定位址範本

指定將套用於此規則的位址範本。下列預先定義的範本包含常見位址選擇。選擇預先定義的範本，或按一下「新增」以自行位址範本：

- 所有 IP 位址**
- 所有 IPv4 位址
- 所有 IPv6 位址
- 所有連結本機 IPv6
- 所有非連結本機 IPv6

新增... 檢視... 刪除

注意：預先定義的範本將建立多項規則。
⚠ 要設定使用 ID 類型為「IP 位址」的 IPsec IKEv2 原則，或設定使用手動金鑰的 IPsec 原則，請建立具特定 IP 位址的位址範本。

【七、電算中心印表機防護處置 - HP-1】

- 強化存取限制：防火牆白名單限定 140.115.XX.0/24

IPsec/防火牆政策

建立位址範本

位址範本名稱
permit 140.115.11.0/24

本機位址

IP 位址
172.20.11.117

預先定義的位址
所有 IPv4 位址

IP 位址範圍
至

IP 位址/首碼 (例如：192.168.1.1/24)
140.115.11.0
24

遠端位址

IP 位址

預先定義的位址
所有 IPv4 位址

IP 位址範圍
至

IP 位址/首碼 (例如：192.168.1.1/24)
140.115.11.0
24

⚠ 注意：多點傳送與廣播位址不受 IPsec 保護

IPsec/防火牆政策

所有 IP 位址
所有 IPv4 位址
所有 IPv6 位址
所有連結本機 IPv6
所有非連結本機 IPv6

permit 140.115.11.0/24

新增... 檢視... 刪除

注意：預先定義的範本將建立多項規則。
⚠ 要設定使用 ID 類型為「IP 位址」的 IPsec IKEv2 原則，或設定使用手動金鑰的 IPsec 原則，請建立具特定 IP 位址的

下一步 >

【七、電算中心印表機防護處置 - HP】

強化存取限制，防火牆白名單限定 140.115.XX.0/24

規則 3：指定服務範本

指定將套用於此規則的服務範本。下列預先定義的範本包含常見服務群組。

服務範本：

- 所有服務
- 所有列印服務
- 所有管理服務
- 所有數位傳送服務
- 所有探索服務

新增... 檢視... 刪除

< 上一步 下一步 > 取消

IPsec/防火牆政策

規則 3：指定動作

您要對流量執行什麼動作以便與位址與服務範本中的準則符合？

- 允許流量通過而不受 IPsec/防火牆保護
- 放棄流量
- 要求流量受 IPsec/防火牆政策保護

< 上一步 下一步 > 取消

IPsec/防火牆政策

| 符合準則 | | 符合動作 | |
|------|------------------------|------|------|
| 規則 | 位址範本 | 服務範本 | 動作 |
| 1 | | | |
| 2 | | | |
| 3 | permit 140.115.11.0/24 | 所有服務 | 允許流量 |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |
| 預設規則 | 所有 IP 位址 | 所有服務 | 放棄 |

< 上一步 建立其他規則 完成 取消

【七、電算中心印表機防護處置 - HP】

- 強化存取限制：防火牆白名單限定 140.115.XX.0/24

IPsec/防火牆政策尚未啟用。
是否要立即啟用此政策？

是 否

是否要啟用故障保護選項？
此選項可確保即使 HTTPS 被 IPsec/防火牆政策封鎖也仍然可以存取。這可讓管理員測試政策，而不會意外地把自己鎖定在裝置外。建議您在成功測試此政策後，停用故障保護選項。

是 否

 變更 IPsec/防火牆設定可能會導致連線暫時中斷。

IPsec/防火牆政策

啟用 IPsec/防火牆

IPsec/防火牆規則

| 規則 | 啟動 | 符合準則 | | 符合動作 |
|----|-------------------------------------|------------------------|--------------|------|
| | | 位址範本 | 服務範本 | 動作 |
| 1 | <input type="checkbox"/> | | | |
| 2 | <input type="checkbox"/> | | | |
| 3 | <input checked="" type="checkbox"/> | permit.140.115.11.0/24 | All Services | 允許流量 |
| 4 | <input type="checkbox"/> | | | |
| 5 | <input type="checkbox"/> | | | |
| 6 | <input type="checkbox"/> | | | |
| 7 | <input type="checkbox"/> | | | |
| 8 | <input type="checkbox"/> | | | |
| 9 | <input type="checkbox"/> | | | |
| 10 | <input type="checkbox"/> | | | |

預設規則 所有 IP 位址 所有服務 放棄

【七、電算中心印表機防護處置 - HP】

- 封鎖攻擊通道：停用 TCP 9100 (DIPRINT / RAW) ，僅開啟 LPR (515) 、IPP (631)

HP Color LaserJet M651
NPIBEE366 172.20.11.117
使用者:Administrator 登出

資訊 一般 列印 耗材 故障排除 安全性 HP Web 服務 **網路**

設定
TCP/IP 設定
網路設定
其它設定
AirPrint
選擇語言
安全
設定
授權
安全通訊
管理通訊協定
802.1X 驗證
IPsec/防火牆
通告代理
診斷
網路統計資料
通訊協定資訊
設定頁

其它設定 說明

其它設定 LPD 佇列 支援資訊 重新整理速率

啟動的功能

| | | |
|---|---|--|
| <input checked="" type="checkbox"/> SLP 設定 | <input checked="" type="checkbox"/> Bonjour | <input checked="" type="checkbox"/> 多點傳送 IPv4 |
| <input type="checkbox"/> 9100 列印 取消勾選 | <input checked="" type="checkbox"/> AirPrint | <input type="checkbox"/> FTP 列印 |
| <input checked="" type="checkbox"/> LPD 列印 | <input checked="" type="checkbox"/> IPP 列印 | <input checked="" type="checkbox"/> IPPS 列印 |
| <input type="checkbox"/> Telnet 設定 | <input checked="" type="checkbox"/> HP Jetdirect XML 服務 | <input checked="" type="checkbox"/> WS-Discovery |
| <input checked="" type="checkbox"/> LLMNR | <input checked="" type="checkbox"/> Web 服務列印 | |
| <input checked="" type="checkbox"/> 啟用 WINS 連接埠 | <input checked="" type="checkbox"/> WINS 註冊 | <input checked="" type="checkbox"/> TFTP 組態檔 |

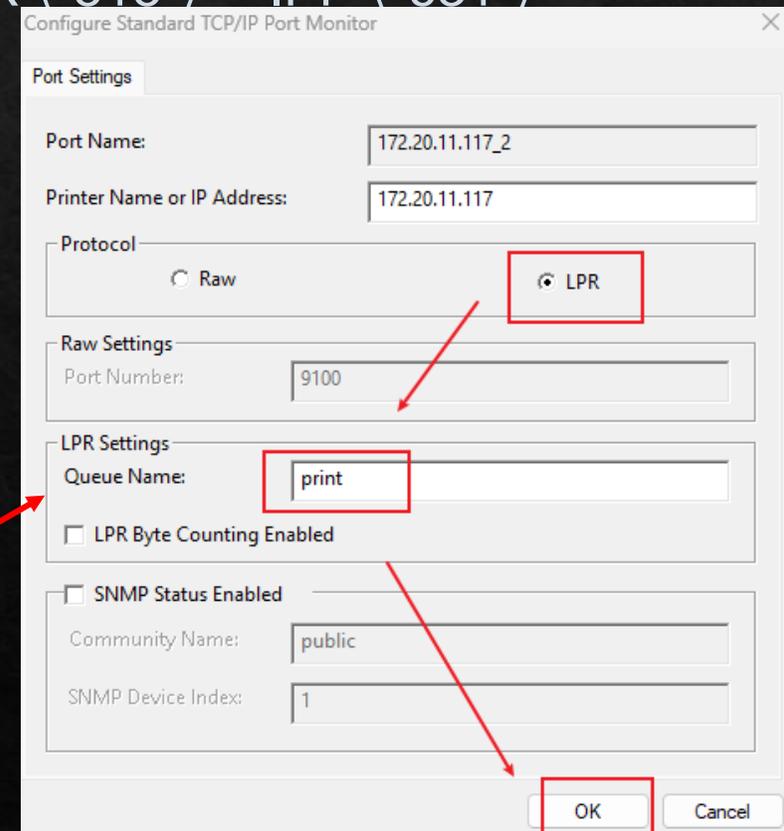
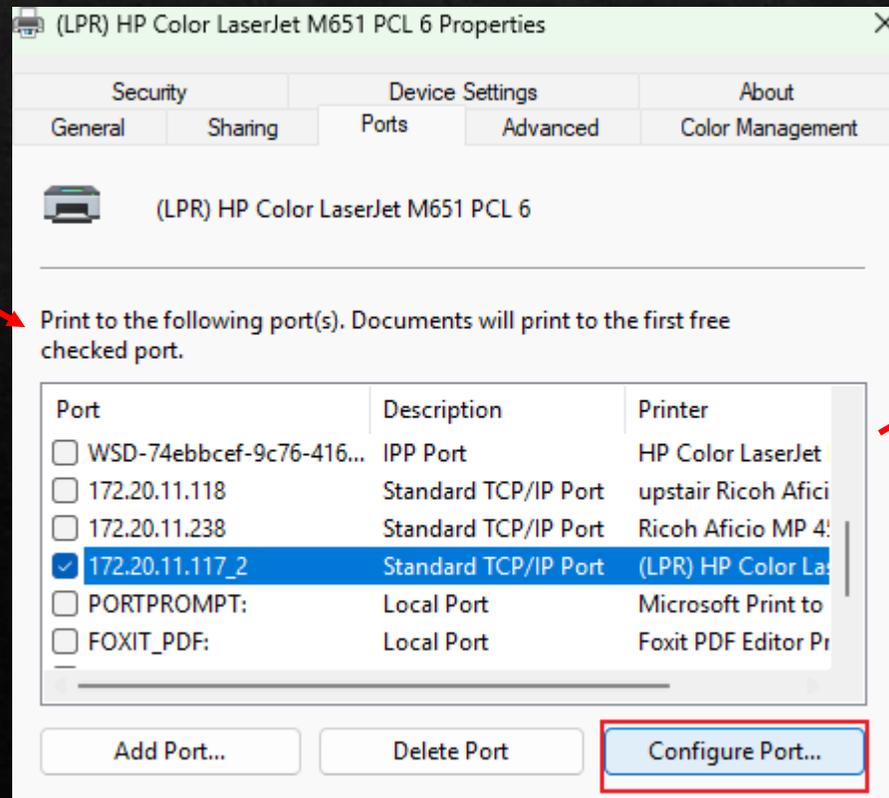
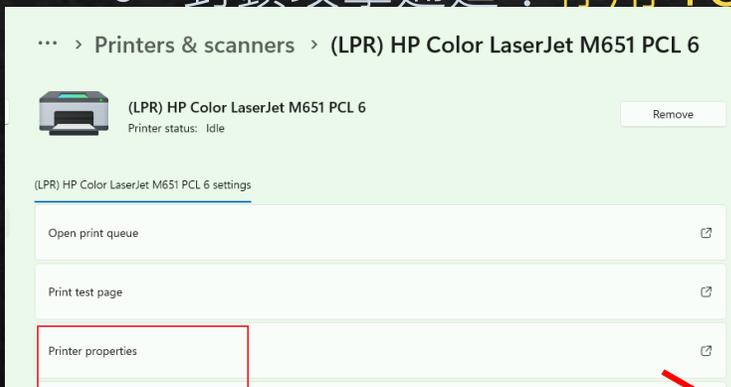
連結設定
自動

本機管理位址
172.20.11.117

套用 取消

【七、電算中心印表機防護處置 - HP】

- 封鎖攻擊通道：停用 TCP 9100 (DIPRINT / RAW) ，僅開啟 LPR (515) 、IPP (631)



【七、電算中心印表機防護處置 - HP】

- 管理介面強化：密碼全面更新至至少10碼，含英文大小寫、數字、特殊符號

hp HP Color LaserJet M651
HP Color LaserJet M651 172.20.11.117

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

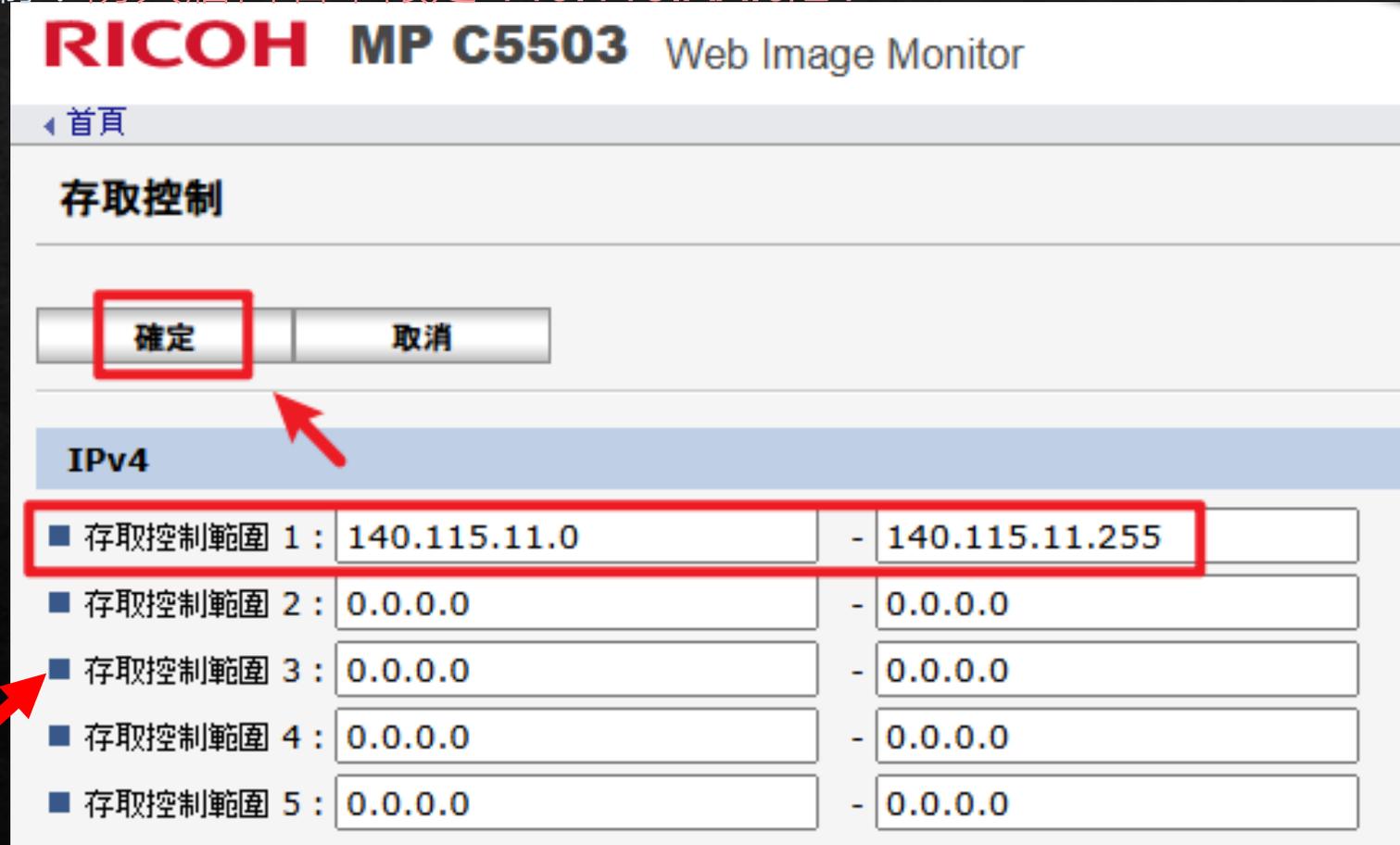
您可以設定管理員密碼，以防止未經授權的使用者從遠端設定裝置或在控制面板上存取為網路管理員保留的功能。此密碼也是裝置的裝置管理員存取碼。

使用者名稱
admin

舊密碼 新密碼 確認密碼

【七、電算中心印表機防護處置 - RICOH】

- 強化存取限制：防火牆白名單限定 140.115.XX.0/24



【七、電算中心印表機防護處置 - RICOH】

- 封鎖攻擊通道：停用 TCP 9100 (DIPRINT / RAW)，僅開啟 LPR (515)、IPP (631)

RICOH MP C5503 Web Image Monitor

◀ 首頁

裝置設定

- 系統
- 功能鍵配置/功能優先
- 紙張
- 日期/時間
- 計時器
- 日誌檔
- 下載日誌檔
- 電子郵件
- 自動電子郵件通知
- 即時電子郵件通知
- 檔案轉送
- 使用者驗證管理
- 管理員驗證的管理
- 登錄/變更管理員
- 列印使用數量限制
- LDAP伺服器
- 韌體更新

介面

- 介面設定

網路

- IPv4
- IPv6
- SMB
- SNMP
- SNMPv3
- SSDP
- Bonjour
- AirPrint
- 系統日誌檔

安全性

- **網路安全性**
- 存取控制

網路安全性

確定 取消

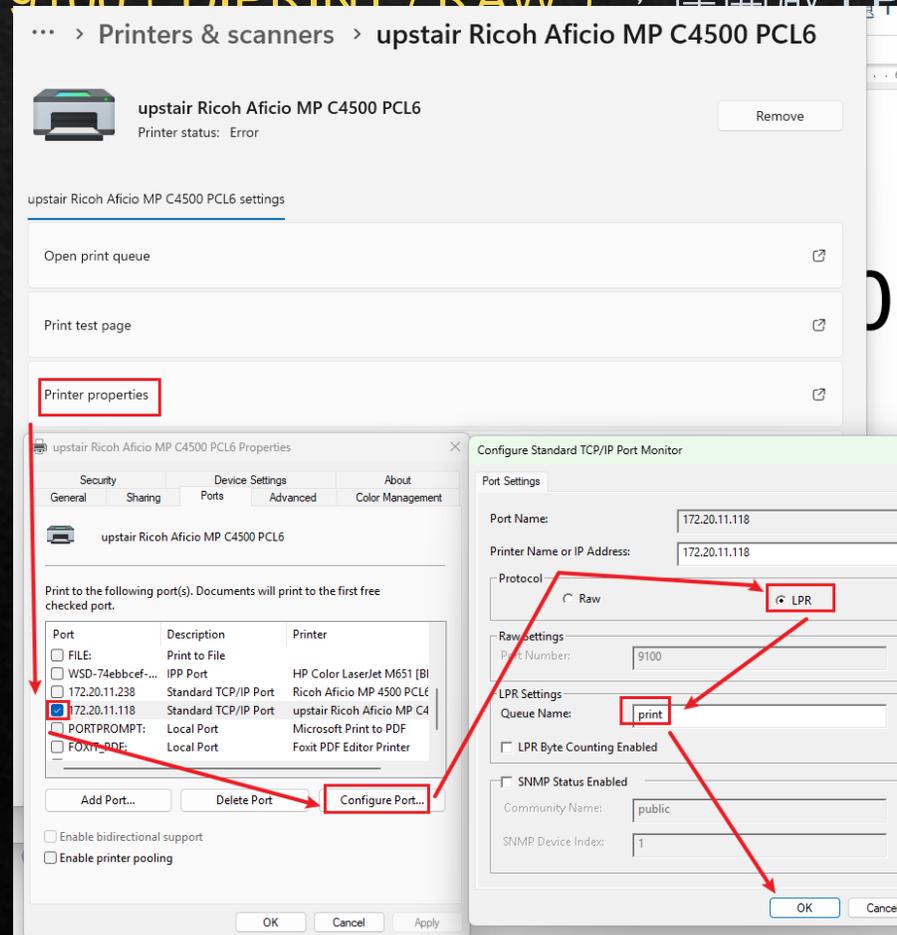
■ 安全性等級 : [使用者設定]

TCP/IP

| | IPv4 | IPv6 |
|------------|--|---|
| TCP/IP | 有效 | <input type="radio"/> 有效 <input checked="" type="radio"/> 無效 |
| HTTP | 連接埠 80 開啟 | <input type="radio"/> 開啟 <input checked="" type="radio"/> 關閉 |
| IPP | 連接埠 80 開啟 | <input type="radio"/> 開啟 <input checked="" type="radio"/> 關閉 |
| | 連接埠 631 <input checked="" type="radio"/> 開啟 <input type="radio"/> 關閉 | <input type="radio"/> 開啟 <input checked="" type="radio"/> 關閉 |
| SSL/TLS | 連接埠 443 <input checked="" type="radio"/> 開啟 <input type="radio"/> 關閉 | <input type="radio"/> 開啟 <input checked="" type="radio"/> 關閉 |
| | 允許 SSL/TLS 通訊 | <input type="text" value="密文/純文字"/> 若要選擇 [僅密文]，必須要有裝置憑證。 |
| | 憑證狀態 | 無 |
| SSL/TLS 版本 | TLS1.2 | <input checked="" type="radio"/> 有效 <input type="radio"/> 無效 |
| | TLS1.1 | <input checked="" type="radio"/> 有效 <input type="radio"/> 無效 |
| | TLS1.0 | <input type="radio"/> 有效 <input checked="" type="radio"/> 無效 |
| | SSL3.0 | <input type="radio"/> 有效 <input checked="" type="radio"/> 無效 |
| 加密強度設定 | AES | <input checked="" type="checkbox"/> 128位元 <input checked="" type="checkbox"/> 256位元 |
| | 3DES | <input type="checkbox"/> 168位元 |
| | RC4 | <input type="checkbox"/> 128位元 |
| | DIPRINT | <input type="radio"/> 有效 <input checked="" type="radio"/> 無效 |
| LPR | <input checked="" type="radio"/> 有效 <input type="radio"/> 無效 | <input type="radio"/> 有效 <input checked="" type="radio"/> 無效 |
| FTP | <input type="radio"/> 有效 <input checked="" type="radio"/> 無效 | <input type="radio"/> 有效 <input checked="" type="radio"/> 無效 |

【七、電算中心印表機防護處置 - RICOH】

- 封鎖攻擊通道：停用 TCP 9100 (DIPRINT / RAW)，僅開啟 LPR (515)、IPP (631)



【七、電算中心印表機防護處置 - RICOH】

- 印表機進行韌體升級 (建議由廠商協助進行)
- http://support.ricoh.com/bb/html/dr_ut_e/rc3/model/r_firm/r_firm.htm

RICOH Firmware Update Tool Ver.1.10.0 Released Date: 02/26/2025 **New!**

Download
(File Size : 5,197 KB)

RICOH Firmware Update Tool allows users to install firmware updates themselves. This tool can be run on Windows OS. It automatically detects the target devices installed on the network that require updates. For a list of supported model, please see: [here](#)

Software

| | | |
|---|--|---|
| <input checked="" type="checkbox"/> Device Manager NX | <input checked="" type="checkbox"/> Printer Driver Packager NX | <input checked="" type="checkbox"/> Printer Driver Editor |
| <input checked="" type="checkbox"/> GlobalScan NX | <input checked="" type="checkbox"/> RICOH Streamline NX | <input checked="" type="checkbox"/> Card Authentication Package |
| <input checked="" type="checkbox"/> Network Device Management | <input checked="" type="checkbox"/> Web SmartDeviceMonitor | <input checked="" type="checkbox"/> Remote Communication Gate S |

Choose other OS

Select driver language: English

Windows

Microsoft Windows 11 (64-bit)

File Explorer window showing the downloaded files:

- z03979en.exe
- CLU_V1.10.0.0 folder containing:
 - RESTSDK.dll
 - RFUT.exe

RICOH Firmware Update Tool

First startup setting
Is this your first time to use RICOH Firmware Update Tool?

Yes
Start RICOH Firmware Update Tool Now

No
Start by migrating data, such as device lists, from the previous version

* Data migration is available on first startup only

OK Cancel

【七、電算中心印表機防護處置 - RICOH】

- 印表機進行韌體升級 (建議由廠商協助進行)

The image displays a sequence of three screenshots from the RICOH Firmware Update Tool, illustrating the process of adding a device for a firmware update. Red arrows indicate the flow from one step to the next.

Environment Setting: The first screenshot shows the 'Environment Setting' dialog box. The 'Operating Environment' tab is active, with 'SNMP Settings' selected. Under 'Proxy Settings', the checkbox 'Use proxy server on LAN(X)' is unchecked. The 'Download Server Select' section has 'Area' set to 'UNITED STATES'. The 'OK' button at the bottom is highlighted with a red box. A red arrow points from this 'OK' button to the 'Specify IP Address' button in the next screenshot.

RICOH Firmware Update Tool: The second screenshot shows the main application window. The 'Specify IP Address' button is highlighted with a red box. A red arrow points from this button to the 'Specify IP Address' dialog box in the next screenshot.

Specify IP Address: This dialog box is titled 'Specify IP Address' and contains the following fields:

- 'Add Device - Manual Entry -'
- 'IP Address or Host Name': 172.20.11.118
- 'Administrator Authentication' section:
 - 'User Name': admin
 - 'Password': *****

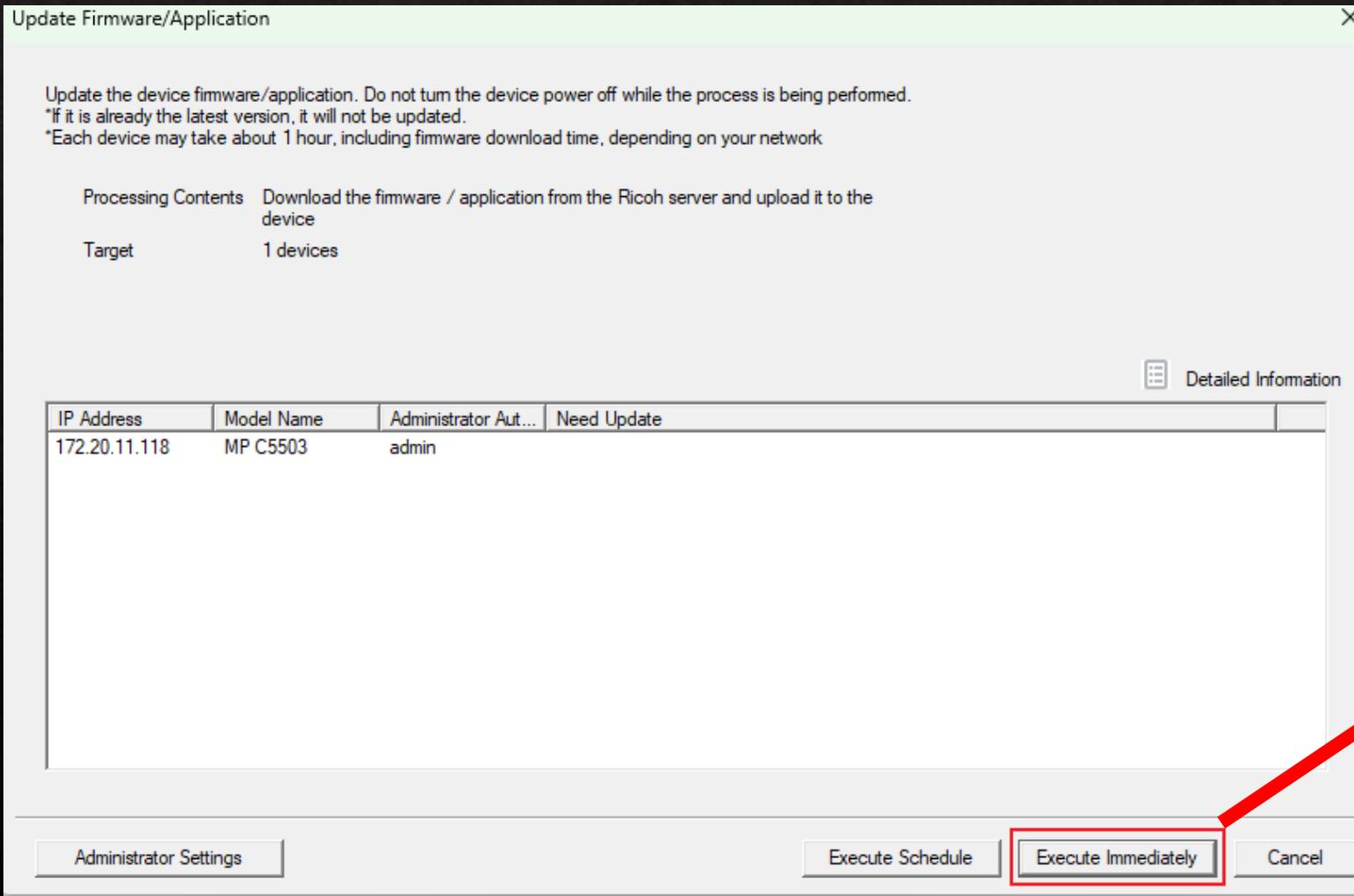
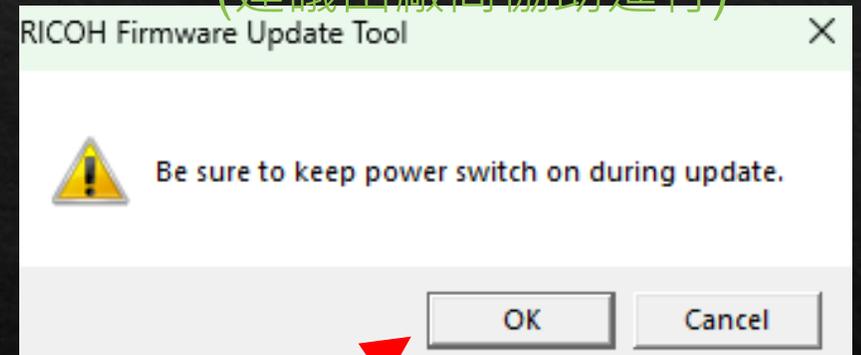
The 'OK' button at the bottom is highlighted with a red box. A red arrow points from this 'OK' button to the 'Adding Devices' dialog box in the next screenshot.

Adding Devices: The third screenshot shows a dialog box titled 'Adding Devices' with the text 'Retrieving device information...'. It features a green progress bar and a 'Cancel' button. A red arrow points from the 'Specify IP Address' dialog box to this dialog.

【七、電算中心印表機防護處置 - RICOH】

- 印表機進行韌體升級

(建議由廠商協助進行)



【七、電算中心印表機防護處置 - RICOH】

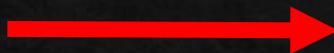
RICOH MP C5503 Web Image Monitor

◀ 首頁

裝置設定

- 系統
- 功能鍵配置/功能優先
- 紙張
- 日期/時間
- 計時器
- 日誌檔
- 下載日誌檔
- 電子郵件
- 自動電子郵件通知
- 即時電子郵件通知
- 檔案轉送
- 使用者驗證管理
- 管理員驗證的管理
- 登錄/變更管理員
- 列印使用數量限制
- LDAP伺服器
- **韌體更新**
- Kerberos驗證

- 印表機進行韌體升級
(建議由廠商協助進行)



韌體版本 更新前

| 模組名稱 | 版本 | 零件編號 |
|-----------------|-----------|-----------|
| System/Copy | 1.40 | D1495569R |
| Network Support | 12.78 | D1495567Y |
| Font EXP | 1.00 | D1495581 |
| PCL Font | 1.06 | D1315586A |
| PS3 Font | 1.12 | D6205681 |
| animation | 7.00 | D1495564D |
| Fax | 15.00.00 | D1495557W |
| RemoteFax | 06.00.00 | D1495558J |
| Printer | 1.20 | D1665701X |
| RPCS | 3.13.24 | D1665703F |
| PCL | 1.20 | D1665706R |
| PDF | 1.05 | D1665733F |
| Scanner | 01.16 | D1495560T |
| NetworkDocBox | 1.05 | D1495568G |
| Web Support | 1.04.9 | D1495561M |
| Web Uapl | 1.04.4 | D1495562G |
| Java VM v11 std | 11.28.03 | D1495579Q |
| PS3 | 1.00 | D1665731A |
| Data Erase Onb | 1.01x | D3775934 |
| GWFCU3.8-2(WW) | 11.00.00 | D1495559M |
| PowerSaving Sys | F.20 | D1495554E |
| Engine | 1.39:08 | D1505504C |
| OpePanel | 1.09 | D1491490K |
| LANG0 | 1.09 | D1491490K |
| LANG1 | 1.09 | D1491490K |
| ADF | 01.340:16 | D6835550F |

韌體版本 更新後 **172.20.11.118**

| 模組名稱 | 版本 | 零件編號 |
|-----------------|-----------|-----------|
| System/Copy | 1.47 | D1495569Y |
| Network Support | 12.83 | D1495565B |
| Font EXP | 1.00 | D1495581 |
| PCL Font | 1.06 | D1315586A |
| PS3 Font | 1.12 | D6205681 |
| animation | 7.00 | D1495564D |
| Fax | 15.00.00 | D1495557W |
| RemoteFax | 06.00.00 | D1495558J |
| Printer | 1.24 | D1665708A |
| RPCS | 3.13.24 | D1665703F |
| PCL | 1.20 | D1665706R |
| PDF | 1.06 | D1665733G |
| Scanner | 01.17 | D1495560V |
| NetworkDocBox | 1.11 | D1495568N |
| Web Support | 1.13 | D1495561Y |
| Web Uapl | 1.07 | D1495562L |
| Java VM v11 std | 11.28.03 | D1495579Q |
| PS3 | 1.00 | D1665731A |
| Data Erase Onb | 1.01x | D3775934 |
| GWFCU3.8-2(WW) | 11.00.00 | D1495559M |
| PowerSaving Sys | F.20 | D1495554E |
| Engine | 1.43:08 | D1505504G |
| OpePanel | 1.09 | D1491490K |
| LANG0 | 1.09 | D1491490K |
| LANG1 | 1.09 | D1491490K |
| ADF | 01.340:16 | D6835550F |

【七、電算中心印表機防護處置 - RICOH】

- 管理介面強化：密碼全面更新至至少10碼，含英文大小寫、數字、特殊符號

RICOH MP C5503 Web Image Monitor

◀ 首頁

裝置設定

- 系統
- 功能鍵配置/功能優先
- 紙張
- 日期/時間
- 計時器
- 日誌檔
- 下載日誌檔
- 電子郵件
- 自動電子郵件通知
- 即時電子郵件通知
- 檔案轉送
- 使用者驗證管理
- 管理員驗證的管理
- **登錄/變更管理員**
- 列印使用數量限制

登錄/變更管理員

確定 取消

- 使用者管理員 : 管理員1 管理員2 管理員3 管理員4
- 機器管理員 : 管理員1 管理員2 管理員3 管理員4
- 網路管理員 : 管理員1 管理員2 管理員3 管理員4
- 檔案管理員 : 管理員1 管理員2 管理員3 管理員4

管理員1

- 登入使用者名稱 : 5566sayHello=.=
- **登入密碼** : **變更**
- 加密密碼 : 變更

變更密碼

[注意] 目前無法使用SSL通訊。下列項目將不經過加密就傳送出去。

- 新密碼 :
- 確認密碼 :

確定 取消

【八、結論與建議】



本事件屬於內部主機遭入侵後，向內網其他設備進行橫向滲透之案例。

本次攻擊行為特徵顯示，懷疑是自動化掃描器（如 `masscan`、`nmap`、`zgrab`）誤將印表機 9100 埠誤認為一般 TCP 服務，套用通用 HTTP 攻擊 payload 進行攻擊，導致印表機列印異常資料。

雖攻擊者未必意識到目標為印表機，但此舉仍暴露出內網存取控管與設備防護的不足，提供了一次檢視現有防護機制的契機。

- 後續建議：
 - 優先落實來源 IP 存取限制，有效縮小內網暴露面。



**THANK YOU
BEARY MUCH!**

NATURALTRIPS.COM