資訊處
Office of Information Technology

設備弱掃後修補建議

中華民國112年10月

編號：

修補主要原則

- 任何設備，如無須對外服務，建議本機端阻擋外部連線，或限制可連線來源
- 個人電腦/筆電/主機，請了解安裝哪些軟體、開啟哪些服務，並確認作業系統與軟體均已更新至最新
- 印表機/無線分享器/監視器等物聯網設備，請確保韌體更新至最新，並完成網路或安全性相關設定

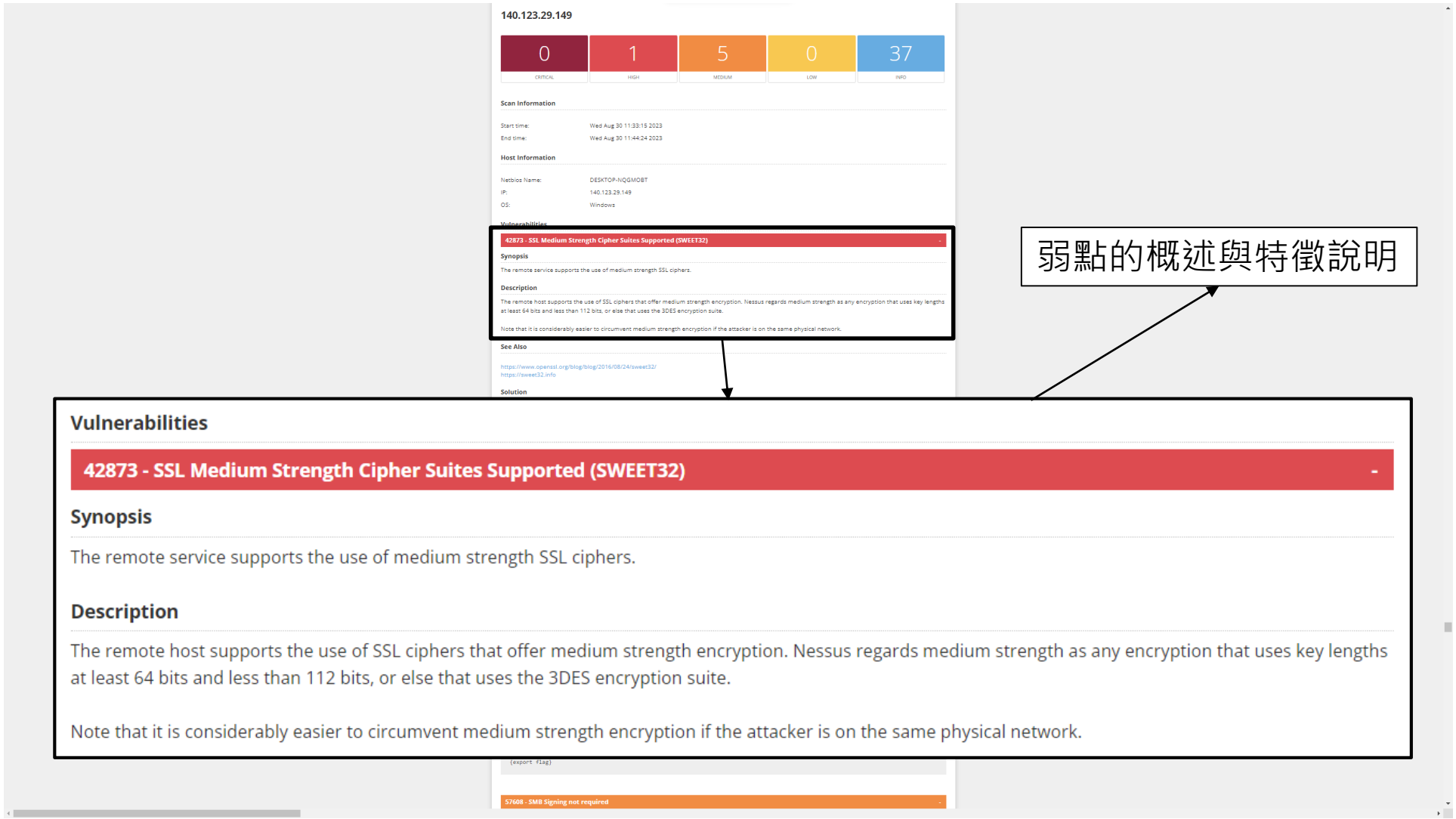
資訊處
Office of Information Technology

如何閱讀報告

風險數統計

統計目標IP弱點數與取得的資訊數
存在Critical(嚴重)、High(高)、Mediun(中)弱點需盡速修補
存在Low(低)弱點僅為建議修補
Info(資訊)為弱掃工具取得該IP設備之服務資訊
目前的共識為中以上弱點都必須修補

弱點名稱與說明


140.123.29.149
0
1
5
0
37
CRITICAL
HIGH
MEDIUM
LOW
INFO
Scan Information
Start time: Wed Aug 30 11:33:15 2023
End time: Wed Aug 30 11:44:24 2023
Host Information
Netbios Name: DESKTOP-NQGMOBT
IP: 140.123.29.149
OS: Windows
Vulnerabilities
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
Synopsis
The remote service supports the use of medium strength SSL ciphers.
Description
The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.
Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.
See Also
https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info
Solution
57608 - SMB Signing not required
弱點的概述與特徵說明
Vulnerabilities
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
Synopsis
The remote service supports the use of medium strength SSL ciphers.
Description
The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.
Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

弱點參考連結與建議修補方式

See Also：提供弱點外部說明參考連結，會有較多針對弱點的特徵說明
Solution：提供弱點修補建議

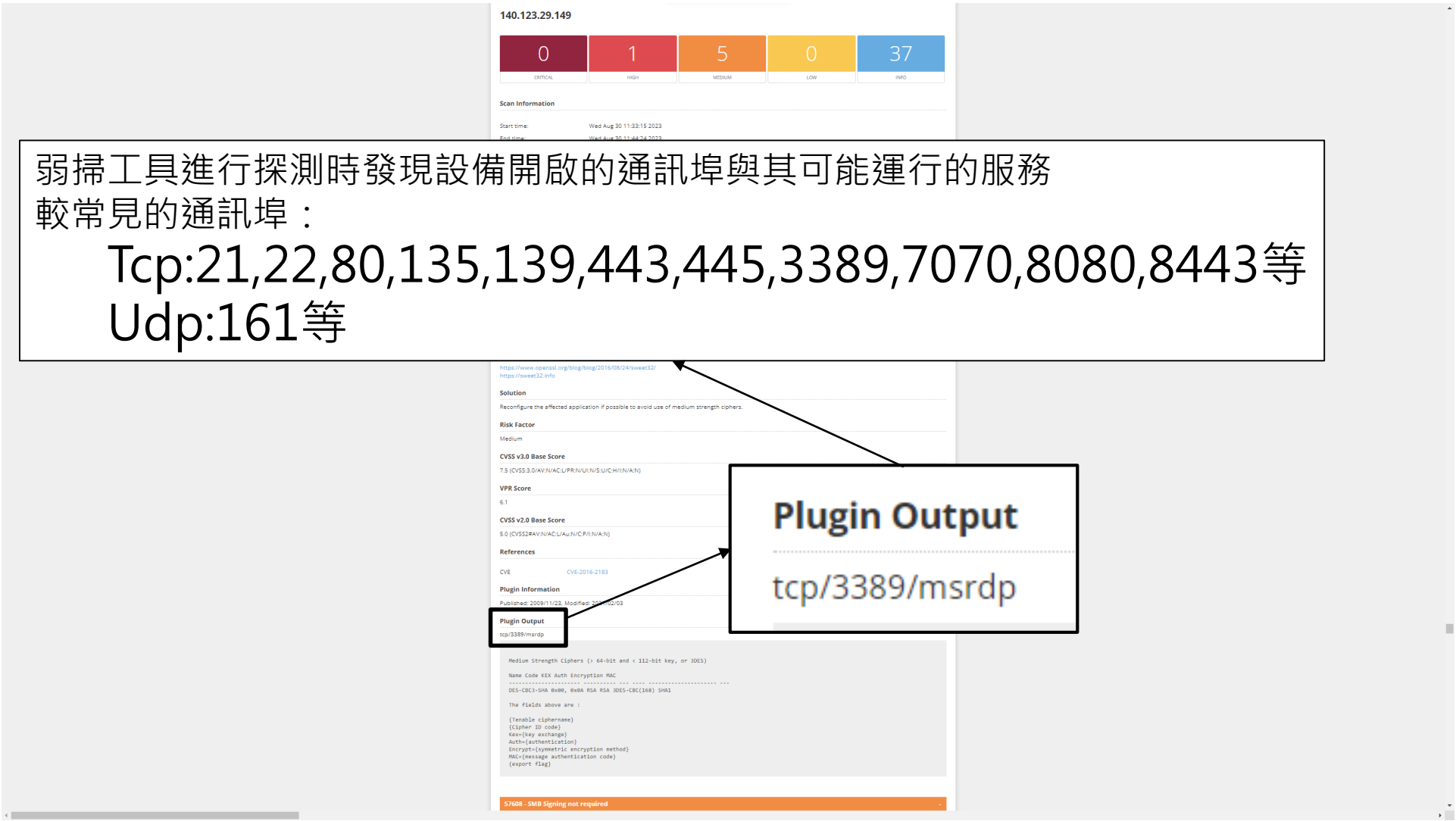
發現弱點的通訊埠

弱掃工具進行探測時發現設備開啟的通訊埠與其可能運行的服務

較常見的通訊埠：

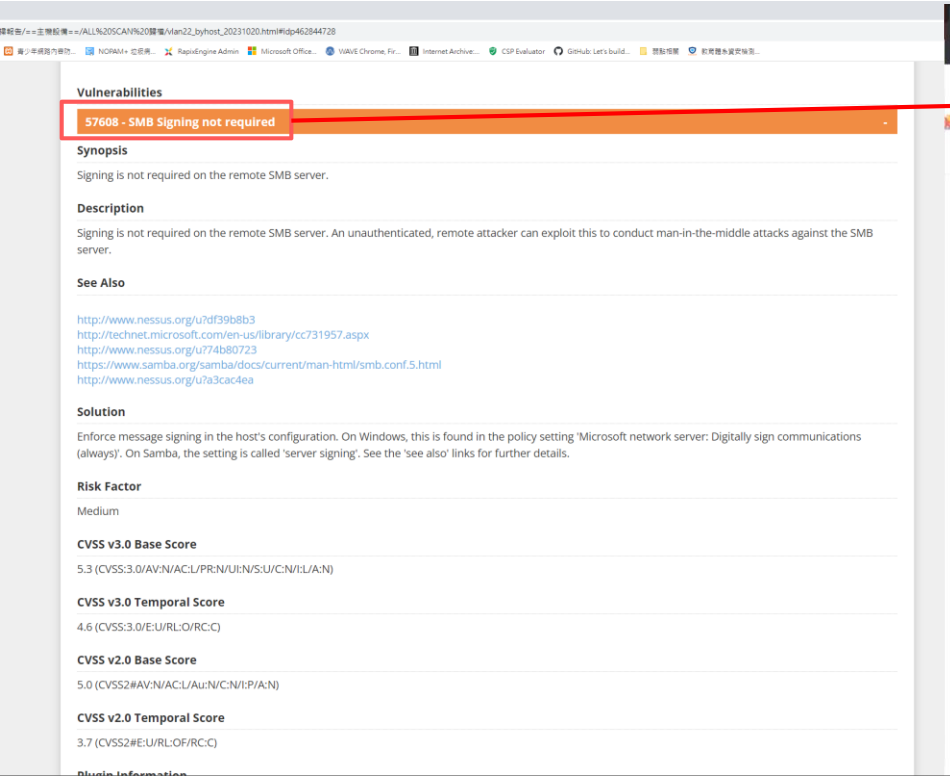
Tcp:21,22,80,135,139,443,445,3389,7070,8080,8443等

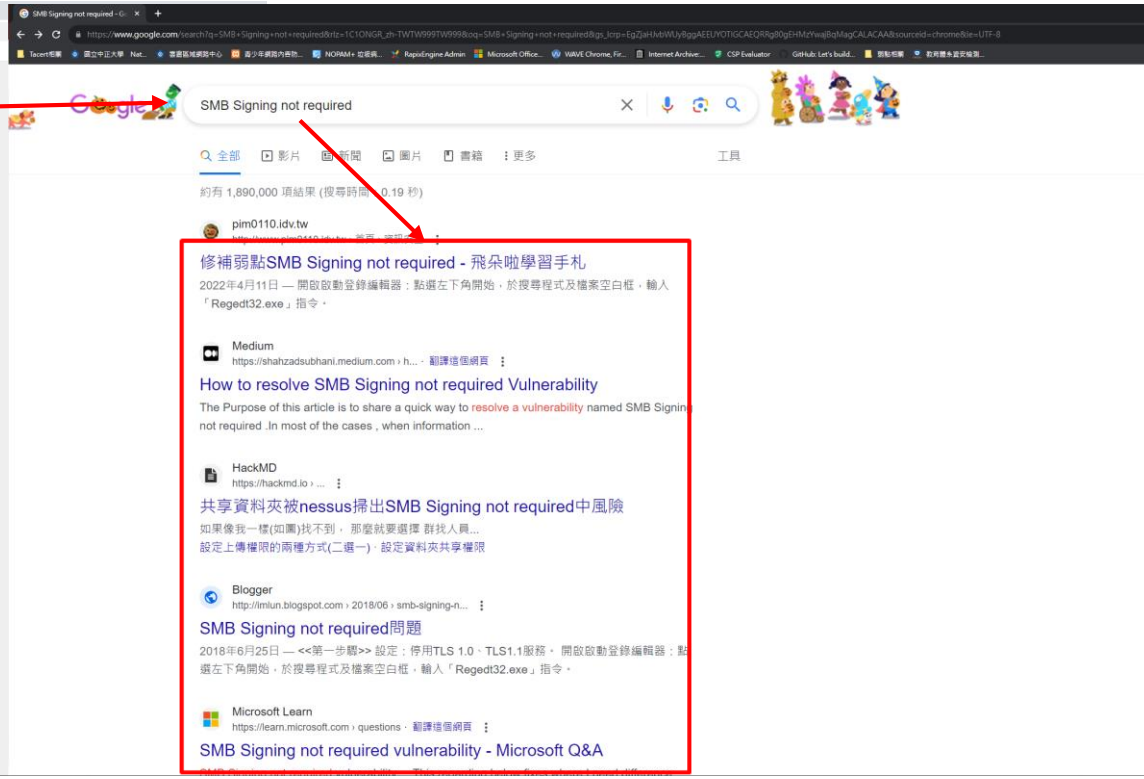
Udp:161等



還是看不懂？

- 請開啟瀏覽器並搜尋弱點名稱，大部分常見的狀況都能找到修補教學





已經搜尋過方法還是無法解決？

- 個人電腦/筆電/主機：
  - ✓建議移除不常使用的軟體或關閉不常使用的服務
  - ✓若無法解決問題，建議重灌設備，一台剛重灌未安裝軟體、未開啟對外服務且也更新到最新的電腦主機，基本上不會有弱點。
- 印表機/無線分享器/監視器等物聯網設備
  - ✓進行設備韌體更新
  - ✓安全性相關設定調校
  - ✓設備網頁管理介面連線存取控制
  - ✓若上述方式都無法進行，請改用私人網段(192.168)、改為單機作業或下架不使用

資訊處
Office of Information Technology

常見弱點項目

51192 - SSL Certificate Cannot Be Trusted

- 若設備為**對外服務**之網站或系統，建議套用有效的SSL憑證
- 目前Let’s Encrypt不被Nessus認為是信任憑證，若為網站或系統使用，本項可視為誤判
- 設備僅為個人或校內特定遠端來源使用，無須對外服務，可以忽略
- 若此弱點出現在tcp 3389，建議本機防火牆限定特定來源，請參閱p21-補充說明1

57582 - SSL Self-Signed Certificate

- 若設備為**對外服務**之網站或系統，建議套用有效的SSL憑證
- 設備僅為個人或校內特定遠端來源使用，無須對外服務，可以忽略
- 若此弱點出現在tcp 3389，建議本機防火牆限定特定來源，請參閱p21-補充說明1

15901 - SSL Certificate Expiry

- 若設備為**對外服務**之網站或系統，建議套用有效的SSL憑證
- 設備僅為個人或校內特定遠端來源使用，無須對外服務，可以忽略
- 若此弱點出現在tcp 3389，建議本機防火牆限定特定來源，請參閱p21-補充說明1

45411 - SSL Certificate with Wrong Hostname

- 若設備為**對外服務**之網站或系統，建議套用有效的SSL憑證
- 設備僅為個人或校內特定遠端來源使用，無須對外服務，可以忽略

104743 - TLS Version 1.0 Protocol Detection

- 若設備為**對外服務**之網站或系統，建議關閉TLS 1.0協定並啟用TLS 1.2以上協定
- 設備請更新系統或韌體至最新
- 若此弱點出現在tcp 3389，建議本機防火牆限定特定來源，請參閱p21-補充說明1
- 若以上方式無法執行，建議設備改用私人網段(192.168.*.*)、改為單機作業或下架不使用

157288 - TLS Version 1.1 Protocol Deprecated

- 若設備為**對外服務**之網站或系統，建議關閉TLS 1.1協定並啟用TLS 1.2以上協定
- 設備請更新系統或韌體至最新
- 若此弱點出現在tcp 3389，建議本機防火牆限定特定來源，請參閱p21-補充說明1
- 若以上方式無法執行，建議設備改用私人網段(192.168.*.*)、改為單機作業或下架不使用

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

- 若設備為**對外服務**之網站或系統，建議套用有效的SSL憑證
- 設備請更新系統或韌體至最新
- 若此弱點出現在tcp 3389，建議本機防火牆限定特定來源，請參閱p21-補充說明1
- 若以上方式無法執行，建議設備改用私人網段(192.168.*.*)、改為單機作業或下架不使用

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

- 若設備為**對外服務**之網站或系統，建議openssl避免使用中強度加密方法
- 設備請更新系統或韌體至最新
- 若此弱點出現在tcp 3389，建議本機防火牆限定特定來源，請參閱p21-補充說明1
- 若以上方式無法執行，建議設備改用私人網段(192.168.*.*)、改為單機作業或下架不使用

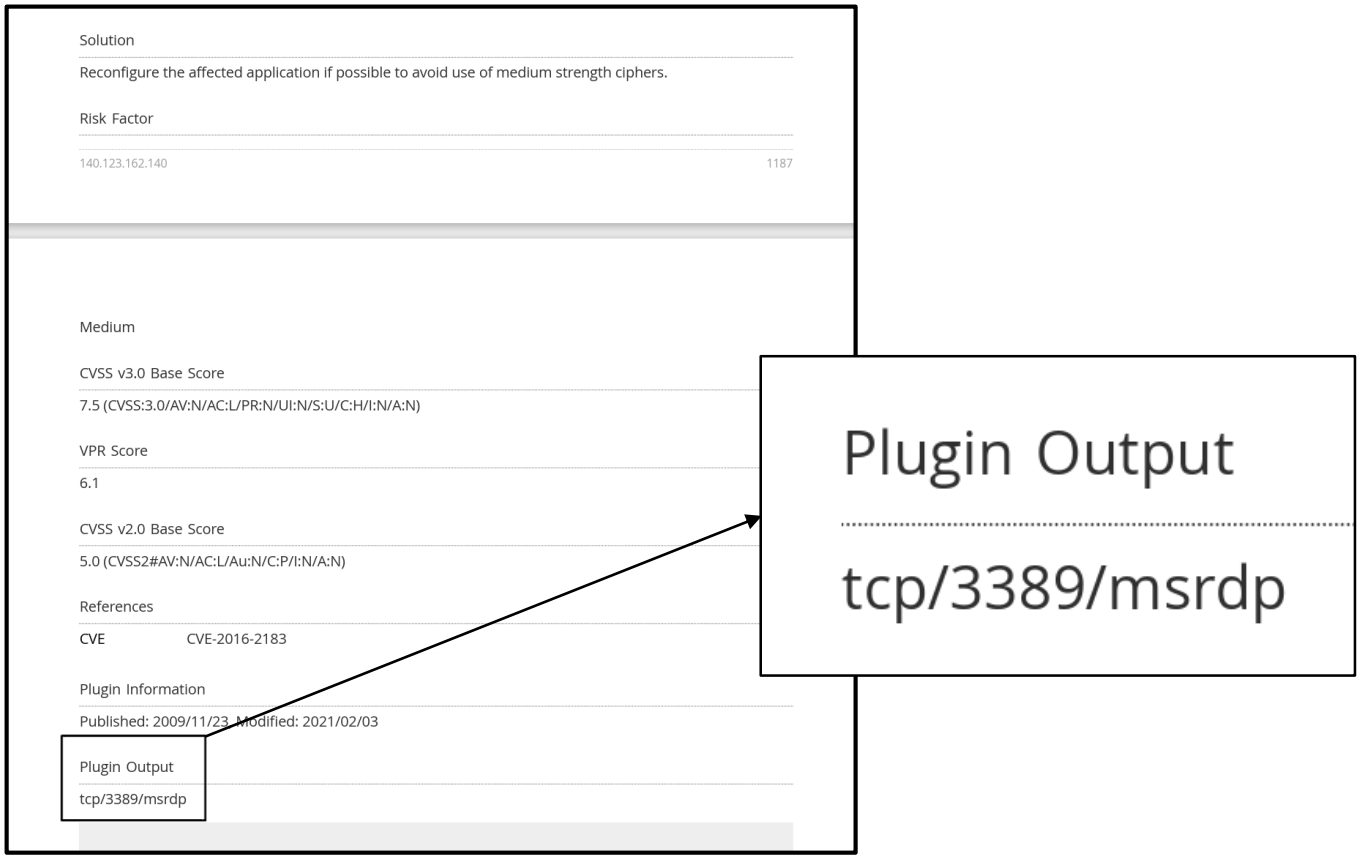
41028 - SNMP Agent Default Community Name (public)

- 如用不到snmp功能，建議**停用**，或更改snmp社群名稱由public改成其他名稱
- 不同廠牌與設備設定不同，建議依產品手冊尋找設定位置，大多會在網路或安全性設定內

- 本項須由設備商釋出更新補丁，若設備商已不支援更新，建議改用私人網段(192.168.*.*)、改為單機作業或下架設備。

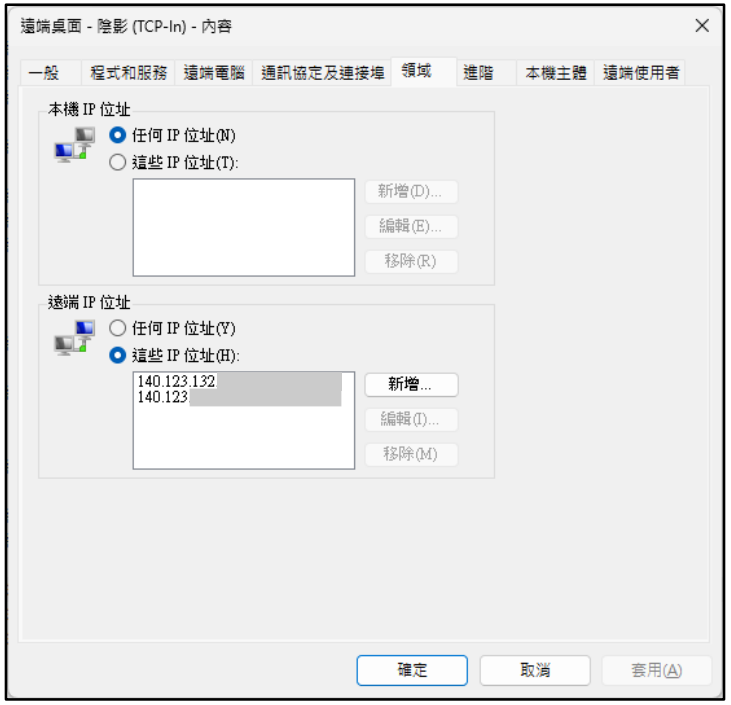
補充說明1 - windows遠端桌面連線

- 先檢查弱點項目的plugin output是否為tcp 3389



補充說明1 - windows遠端桌面連線

- 參考資訊處手冊p17~p27
- https://it.ccu.edu.tw/var/file/9/1009/img/Remote_Working_0607.pdf
- 建議依照手冊流程設定遠端來源IP-140.123.132.0/24或特定IP
- 學生vpn請設定140.123.3.0/24或特定IP



資訊處
Office of Information Technology

感謝閱讀