# 政府組態基準
# Juniper Firewall
# (V1.1)

行政院國家資通安全會報技術服務中心
中華民國108年12月

# 修訂歷史紀錄表

| 項次 | 版次 | 修訂日期 | 說明 |
|---|---|---|---|
| 1 | 1.0 | 106/1/12 | 新編 |
| 2 | 1.1 | 108/12/17 | ▪ 新增「TWGCB-ID」欄位與資料<br>▪ 調整表 2「GCB 設定值」欄位順序 |
| 3 | | | |
| 4 | | | |
| 5 | | | |

# 目次

1. 前言 ..... 1
1.1. 適用環境 ..... 1
1.2. 項數統計 ..... 1
1.3. 文件發行 ..... 2
2. Juniper Firewall 設備政府組態基準列表 ..... 3
3. 參考文獻 ..... 20

# 表 目 次

表 1　Juniper Firewall 設備組態基準項目統計 ..... 1
表 2　Juniper Firewall 設備政府組態基準列表 ..... 3

## 1. 前言

政府組態基準(Government Configuration Baseline, 以下簡稱 GCB)目的在於規範資通訊終端設備(如：個人電腦)的一致性安全設定(如：密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之疑慮。

### 1.1.適用環境

本文件適用於 Juniper Firewall 設備，JUNOS 版本 8.x / 9.x / 10.x 版本。

### 1.2.項數統計

政府組態基準針對電腦作業環境提供一致性安全基準與實作指引，供政府機關透過建立安全組態，提升資安防護能力。Juniper Firewall 設備組態基準計有 49 項設定項目，項目統計詳見表 1。

表1　Juniper Firewall 設備組態基準項目統計

| 項次 | 類別 | 項數 | 合計 |
|---|---|---|---|
| 1 | Interface | 2 | 49 |
| 2 | SNMP | 8 | |
| 3 | Diag-Port-Authentication | 2 | |
| 4 | Login | 12 | |
| 5 | NTP | 1 | |
| 6 | Root-Authentication | 3 | |
| 7 | Services | 12 | |
| 8 | Ports | 1 | |
| 9 | SYSLOG FILE | 2 | |
| 10 | Miscellaneous System Settings | 6 | |

資料來源：本中心整理

### 1.3.文件發行

本文件最新版本公布於本中心網站之「政府組態基準」專區，網址為 https://www.nccst.nat.gov.tw/GCB。

## 2. Juniper Firewall 設備政府組態基準列表

表2　Juniper Firewall 設備政府組態基準列表

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB設定值 | 備註 |
|---|---|---|---|---|---|---|---|
| 1 | TWGCB-03-002-0001 | Interfaces | 關閉未使用的介面 | 為了確保未使用的介面端口不會意外連接到網絡，或者受到惡意攻擊者試圖繞過安全措施，應禁用所有未使用的介面端口 | [edit interfaces <interface name>]<br>user@host#set disable | 關閉未使用介面 | |
| 2 | TWGCB-03-002-0002 | | 需要設置介面描述 | 為了提高網路規劃的效率，並有效針進行故障排除，及避免可能危及網絡安全的混亂和錯誤，所有介面應配置相關的描述說明 | [edit interfaces <interface name> unit <unit number>]<br>user@host#set description <description> | 設置介面描述 | |
| 3 | TWGCB-03-002-0003 | SNMP | 禁止常見的 SNMP 通用字串 | 當使用 SNMPv2c 版本時，可利用通用字串進行管理行為，若攻擊者猜測到所使用的通用字串時，可能會存取 SNMP 介面，就像合法管理者一樣 | [edit snmp]<br>user@host#rename community <old community> to community <new community> | 禁用 SNMP 通用字串 | |

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB設定值 | 備註 |
|---|---|---|---|---|---|---|---|
| 4 | TWGCB-03-002-0004 | | 限制 SNMP v1, v2 及 v2c 的寫入功能 | SNMP 可以利用網路管理的方式針對設備進行設定檔的寫入或讀取，並且舊的 SNMP 版本 v1、v2 和 v2C 存在不安全的明碼傳輸設計，使得容易遭受攻擊者擷取傳輸資訊進而取得通用字串內容 | [edit snmp]<br>user@host#delete community <community><br>[edit snmp <community>]<br>user@host#set authorization read-only | 限制寫入功能 | |
| 5 | TWGCB-03-002-0005 | | 需要 SNMPv1 和 SNMPv2 的端點列表 | 即使僅限 Read-Only 存取，攻擊者還是可能透過 SNMP 取得有關網路設備和網絡拓撲的大量訊息。為了降低網路設備 SNMP 服務的攻擊利用可能性，應限制僅有使用者端列表的 IP 位置進行連線 | [edit snmp]<br>user@host#edit client-list <client list name><br>[edit snmp client-list <client list name>]<br>user@host#set default restrict<br>user@host#set <ip address><br>user@host#set <ip address> restrict #optionally add exceptions<br>user@host#up 1 | 設置端點列表 | |

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB設定值 | 備註 |
|---|---|---|---|---|---|---|---|
| | | | | | [edit snmp]<br>user@host#edit community <community name><br>[edit snmp community <community name>]<br>user@host#set client-list-name <client list name> | | |
| 6 | TWGCB-03-002-0006 | | 需要SNMP端點列表的Default Restrict | 即使僅限Read-Only存取，攻擊者還是可能透過SNMP取得有關網路設備和網絡拓撲的大量訊息。為了降低網路設備SNMP服務的攻擊利用可能性，應拒絕未被加入使用者端列表的IP位置進行連線 | [edit snmp client-list <client list name>]<br>user@host#set default restrict | 設置Default Restrict | |
| 7 | TWGCB-03-002-0007 | | 限制SNMP的寫入功能 | SNMP可以利用網路管理的方式針對設備進行設定檔的寫入或讀取，並且舊的SNMP版本v1、v2和v2C存在不安全的明碼傳輸設計，使得容易遭受 | [edit snmp]<br>user@host#delete community <community><br>[edit snmp v3 vacm access] | 限制寫入功能 | |

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB設定值 | 備註 |
|---|---|---|---|---|---|---|---|
| | | | | 攻擊者擷取傳輸資訊進而取得通用字串內容 | user@host#delete group <group name> default-context-prefix security-model <security model> security-level <security level> write-view | | |
| 8 | TWGCB-03-002-0008 | | 需要以AES128加密的SNMP存取 | SNMPv3提供訊息驗證和加密功能，比以前版本具有更高安全性，當中最高加密方式可採用AES128 | [edit snmp v3 usm local-engine] user@host#set user <username> privacy-aes128 privacy-password <password> | 設置AES128加密 | |
| 9 | TWGCB-03-002-0009 | | 需要以SHA驗證SNMPv3的存取 | SNMPv3使用的驗證方式是Keyed-Hash Message或是HMAC，利用這種技術進行驗證並確保訊息的完整性。JUNOS在SNMPv3使用的驗證方式是MD5和SHA1，MD5屬於較舊的協議，近年來已經存在相關的脆弱 | [edit snmp v3 usm local-engine] user@host#set user <username> authentication-sha | 設置SHA存取 | |

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB設定值 | 備註 |
|---|---|---|---|---|---|---|---|
| | | | | 性，因此應使用較新和較值得信賴的SHA1 方式 | <password> | | |
| 10 | TWGCB-03-002-0010 | | 需要SNMP的使用介面限制 | 預設狀態下 SNMP 服務將針對所有配置 IP 地址的介面進行連入監聽，並向可存取設備的來源提供 SNMP，但網路設備應只能通過某些介面進行管理，特別是在不可信任的網絡(Internet)中，連接的來源應被管理 | [edit snmp]<br>user@host#set interface <interface or interface list> | 限制SNMP使用介面 | |
| 11 | TWGCB-03-002-0011 | Diag-Port-Authentication | 需要偵錯埠的身分驗證 | 大部分的 Juniper 設備具有一個或多個偵錯埠，攻擊者可以透過實體入侵的方式，利用偵錯埠來進行惡意行為，為了避免這種風險，可為設備的偵錯埠設置密碼驗證 | [edit system]<br>user@host#set diag-port-authentication plain-text-password<br>[edit system]<br>user@host#set diag-port-authentication encrypted-password "<MD5 Hash>" | 設置身分驗證 | |

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB設定值 | 備註 |
|---|---|---|---|---|---|---|---|
| 12 | TWGCB-03-002-0012 | | 偵錯埠需具複雜性的密碼原則 | 應使用複雜的密碼組合，以降低攻擊者透過暴力破解或字典檔攻擊等方式的成功機率 | [edit system]<br>user@host#set diag-port-authentication plain-text-password<br>[edit system]<br>user@host#set diag-port-authentication encrypted-password "<MD5 Hash>" | 設置密碼複雜原則 | |
| 13 | TWGCB-03-002-0013 | Login | 需要建立所有使用者帳號的登入類別 | 為網路設備設置使用者存取類別，可降低因惡意或失誤的操作行為，而導致錯誤設定所造成的風險 | [edit system login]<br>user@host#set user <username> class <class name> | 設置帳戶登入類別 | |
| 14 | TWGCB-03-002-0014 | | 需要建立所有登入類別的閒置逾時 | 所有的登入類型皆應設置 15 分鐘內的閒置逾時功能，以避免無人使用的 Session 佔用連線資源 | [edit system login]<br>user@host#set class <class name> idle-timeout <timeout in minutes> | 設置閒置逾時 | |

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB設定值 | 備註 |
|---|---|---|---|---|---|---|---|
| 15 | TWGCB-03-002-0015 | | 需要建立所有登入類別的權限級別 | 登入類別應授予不同的權限，以避免惡意或失誤的操作，而導致錯誤設定所造成的風險 | [edit system login] user@host#set class <class name> permissions <permission or list of permissions> | 設置登入權限級別 | |
| 16 | TWGCB-03-002-0016 | | 限制所有登入類別使用 Shell 存取 | 某些權限可能能夠透過 Shell 直接與底層系統互動，但為了確保設備的行為必須透過 JUNOS 執行，所有登入類別的存取行為應拒絕透過 Shell 執行 | [edit system login] user@host#set class <class name> deny-commands "start shell" | 限制 Shell 存取 | |
| 17 | TWGCB-03-002-0017 | | 限制所有使用者帳號採用預設登入類別 | 預設的登入類別雖然提供基本的設定，但無法符合安全性選項的建議，因此不應使用預設登入類別來進行使用權限授權 | [edit system login] user@host#set user <username> class <class name> | 限制預設登入類別 | |
| 18 | TWGCB-03-002-0018 | | 需要登入訊息 | 透過登入訊息提醒使用者相關的法律責任與資安政策等資訊 | [edit system] user@host#set login message "<LEGAL | 設置登入訊息 | |

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB設定值 | 備註 |
|---|---|---|---|---|---|---|---|
| | | | | | NOTICE>" | | |
| 19 | TWGCB-03-002-0019 | | 密碼需要具有多種字元符號 | 應使用複雜的密碼組合，以降低攻擊者透過暴力破解或字典檔攻擊等方式的成功機率 | [edit system]<br>user@host#set login password change-type character-set | 設置密碼複雜組合 | |
| 20 | TWGCB-03-002-0020 | | 密碼需要最少4種不同的字元符號 | 過於簡短的密碼組合方式，容易遭受攻擊者猜測破解，安全的密碼應包含至少4個不同字元符號組合，如大寫字母，小寫字母，數字，標點符號和特殊字符等 | [edit system]<br>user@host#set login passwords minimum-changes 4 | 設置4種密碼複雜組合 | |
| 21 | TWGCB-03-002-0021 | | 密碼需要最少8碼的字元長度 | 過於簡短的密碼組合方式，容易遭受攻擊者猜測破解，安全的密碼至少應採用8碼以上的字元長度 | [edit system]<br>user@host#set login passwords minimum-length 8 | 設置密碼8字元以上 | |
| 22 | TWGCB-03-002-0022 | | 密碼需要SHA1的加密保存 | 採用SHA1的方式保存密碼，以避免攻擊者直接從系統資料中讀取密碼內容 | [edit system]<br>user@host#set login password format sha1 | 設置SHA1密碼加 | |

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB設定值 | 備註 |
|---|---|---|---|---|---|---|---|
| | | | | | | 密 | |
| 23 | TWGCB-03-002-0023 | | 中斷連線前允許最多3次的嘗試 | 針對 Telnet 或 SSH 等遠端管理協定，為了降低暴力破解的速度，應限制在 3 次以下的登入嘗試失敗後，中斷連線 | [edit system]<br>user@host#set login retry-options tries-before-disconnect <number of tries> | 設置 3 次連線失敗嘗試限制 | |
| 24 | TWGCB-03-002-0024 | | 需要最少 20 秒的 Session 時間 | 針對 Telnet 或 SSH 等遠端管理協定，為了降低暴力破解的速度，應限制 Sessions 的最少時間為 20 秒以上，以防止攻擊者嘗試透過多個 Sessions 的方式來規避登入控管機制 | [edit system]<br>user@host#set login retry-options minimum-time 20 | 設置 20 秒以上的 Session 時間 | |
| 25 | TWGCB-03-002-0025 | NTP | 需要外部時間來源 | 為了確保日誌數據的有效性，及釐清故障或安全事件發生的時間點，應設置至少 2 個以上的 NTP 伺服器 | [edit system]<br>user@host#set ntp server <Servers IP> key <key ID> version 4 | 設置 NTP 伺服器位置 | |
| 26 | TWGCB-03-002- | Root-Authenticatio | 需要 Root 密碼 | 應設置強密碼來限制存取 Root 帳戶，密碼的設定內容應加密保存，以防止 | [edit system]<br>user@host#set | 設置 Root 密 | |

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB設定值 | 備註 |
|---|---|---|---|---|---|---|---|
| | 0026 | n | | 從備份或其他來源顯示 | root-authentication plain-text-password user@host#set root-authentication encrypted-password "<SHA1 hash>" | 碼 | |
| 27 | TWGCB-03-002-0027 | | 需要複雜原則的Root 密碼 | 應使用複雜的密碼組合，以降低攻擊者透過暴力破解或字典檔攻擊等方式的成功機率 | [edit system] user@host#set root-authentication plain-text-password user@host#set root-authentication encrypted-password "<SHA1 hash>" | 設置Root 密碼複雜原則 | |
| 28 | TWGCB-03-002-0028 | | 需要唯一的 Root 密碼 | 為了保護 Root 帳戶的安全，應避免使用與其他帳戶相同或類似的密碼內容，以避免攻擊者可透過其他密碼資 | [edit system] user@host#set root-authentication plain-text-password | 設置唯一 Root 密碼 | |

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB設定值 | 備註 |
|---|---|---|---|---|---|---|---|
| | | | | 訊猜測出 Root 帳戶所使用的密碼內容 | user@host#set root-authentication encrypted-password "<SHA1 hash>" | | |
| 29 | TWGCB-03-002-0029 | Services | 限制使用 Telnet 服務 | 由於 Telnet 透過網路以明文傳輸所有數據（包括密碼），並且不能保證連線主機的身份，因此可能會遭受攻擊者獲取機敏資訊，也容易受到 Session 劫持和中間人攻擊。為了避免這種風險的發生，應限制使用 Telnet 服務 | [edit system] user@host#delete services telnet | 限制 Telnet 服務 | |
| 30 | TWGCB-03-002-0030 | | 限制使用 FTP 服務 | 由於 FTP 使用明文方式傳輸資料，應禁止使用或以 SSH 方式取代，以避免遭受攻擊者從中竊取機敏資料 | [edit system] user@host#delete services ftp | 限制 FTP 服務 | |
| 31 | TWGCB-03-002-0031 | | 需要使用 SSH 服務 | SSH 以類似於 Telnet 的方式為管理員提供網路設備的遠端控制台連線，但與 Telnet 不同的是 SSH 在傳輸時會加密所有數據，並確保遠端主機的身 | [edit system] user@host#set services ssh | 設置 SSH 服務 | |

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB設定值 | 備註 |
|---|---|---|---|---|---|---|---|
| | | | | 份，由於這個保護的機制，所有遠端控制台應該使用 SSH 連線 | | | |
| 32 | TWGCB-03-002-0032 | | 需要使用 SSHv2 | 由於 SSHv1 版本存在許多的安全問題，應使用更加安全的 SSHv2 版本 | [edit system]<br>user@host#set services ssh protocol-version v2 | 設置 SSHv2 | |
| 33 | TWGCB-03-002-0033 | | 需要限制 SSH 連線 | 攻擊者經常將 SSH 服務作為阻斷服務的攻擊目標，為了降低阻斷服務攻擊和暴力破解攻擊的有效性，應限制 SSH 連線的最大數量，通常會限制最大為 10 個的連線 Sessions | [edit system]<br>user@host#set services ssh connection-limit <limit> | 限制 SSH 連線數量 | |
| 34 | TWGCB-03-002-0034 | | 需要限制 SSH 速率 | 攻擊者經常將 SSH 服務作為阻斷服務的攻擊目標，為了降低阻斷服務攻擊和暴力破解攻擊的有效性，應限制每秒連線速率，通常會限制每秒 4 個新的連線 Sesssions | [edit system]<br>user@host#set services ssh rate-limit <limit> | 限制 SSH 連線速率 | |
| 35 | TWGCB-03-002- | | 限制遠端存取 Root | 因 Root 帳戶具有底層作業系統的完整存取權限，所以對攻擊者而言是非常 | [edit system]<br>user@host#set services ssh | 限制 Root 帳 | |

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB設定值 | 備註 |
|---|---|---|---|---|---|---|---|
| | 0035 | | 帳戶 | 有價值的攻擊目標，故應限制透過遠端連線進行存取，並確保僅能透過實體連線的方式進行使用 | root-login deny | 戶遠端登入 | |
| 36 | TWGCB-03-002-0036 | | 當安裝了JWEB服務，避免以HTTP方式存取 | 因HTTP以明文形式傳輸所有數據(包括密碼），並且不能確保連線主機的身份，故不應用於管理網路設備 | [edit system] user@host#delete services web-management http | 限制已HTTP存取 | |
| 37 | TWGCB-03-002-0037 | | 當安裝了JWEB服務，需要以HTTPS方式存取 | 因HTTPS使用SSL加密所有數據，並使用憑證確連線主機的身份，故建議可以此方式管理網路設備 | [edit system] user@host#set services web-management https local-certificate <certificate name> | 設置HTTPS存取 | |
| 38 | TWGCB-03-002-0038 | | 當安裝了JWEB服務，需要設置連線逾 | 為了避免閒置的管理Sessions被攻擊者所利用，應限制當Sessions閒置15分鐘以上即中斷連線 | [edit system] user@host#set services web-management session idle-timeout <Time in | 設置連線逾時 | |

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB設定值 | 備註 |
|---|---|---|---|---|---|---|---|
| | | | 時 | | Minutes> | | |
| 39 | TWGCB-03-002-0039 | | 當安裝了JWEB服務，需要限制Session數量 | 為了避免攻擊者利用打開大量的JWEB Sessions嘗試耗盡設備資源，應限制JWEB Session的最大數量為5以下 | [edit system]<br>user@host#set services web-management session session-limit 5 | 限制5個以下的Session數量 | |
| 40 | TWGCB-03-002-0040 | | 當安裝了JWEB服務，需要存取介面限制 | 預設狀態下JWEB服務將針對所有配置IP地址的介面進行連入監聽，並向可存取設備的來源提供服務，但網路設備應只能通過某些介面進行管理，特別是在不可信任的網絡(internet)中，連接的來源應被管理 | [edit system services web-management https]<br>user@host#set interface <interface or interface list> | 限制存取介面 | |
| 41 | TWGCB-03-002-0041 | Ports | 結束連線立刻關閉控制Session | 當設備管理員使用實體的Console介面進行管理時，若將線路拔除時，控制台的Sessions可能會保持登入狀態，以供下一次管理設定使用，但為了避免攻擊者利用此狀況進行非授權 | [edit system]<br>user@host#set ports console log-out-on-disconnect | 設置連線結束關閉Session | |

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB設定值 | 備註 |
|---|---|---|---|---|---|---|---|
| | | | | 存取使用，應設置一旦移除連線則立即關閉控制台的 Sessions | | | |
| 42 | TWGCB-03-002-0042 | SYSLOG FILE | 所有的身分證驗與授權行為需要本機端的 SYSLOG 紀錄 | 當使用者進行登入或執行需要授權操作行為(例如更改設定)時，應紀錄相關事件 LOG 資料，以利後續需進行故障排除或事件追蹤時，可加以利用 | [edit system syslog] user@host#set file <filename> authorization any | 設置身分驗證與授權行為 Syslog | |
| 43 | TWGCB-03-002-0043 | | 所有的互動式命令需要本機端的 SYSLOG 紀錄 | 當系統發生故障或資安警訊事件時，應紀錄相關事件 LOG 資料，以利後續進行事故排除或事件追蹤 | [edit system syslog] user@host#set file <filename> interactive-commands any | 設置互動式命令 Syslog | |
| 44 | TWGCB-03-002- | Miscellaneous | 設定檔需要加密保 | 為了避免攻擊者透過明文的設定檔內容中找出機敏的資訊，應將設定檔內 | [edit] user@host>request system | 設置設定檔加 | |

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB設定值 | 備註 |
|---|---|---|---|---|---|---|---|
| | 0044 | System Settings | 存 | 容以加密方式保存 | set-encryption-key<br>[edit system]<br>user@host#set<br>encrypt-configuration-files | 密 | |
| 45 | TWGCB-03-002-0045 | | 忽略多點廣播的回應請求 | 攻擊者可透過多點廣播請求的方式蒐集網路設備列表及所提供的服務資訊，因此若不需使用此功能，則應將其關閉 | [edit system]<br>user@host#set<br>no-multicast-echo | 限制多點廣播回應請求 | |
| 46 | TWGCB-03-002-0046 | | 關閉 Ping 的路由紀錄回應請求 | 攻擊者可利用 Ping 的路由紀錄獲取網路拓樸等資訊，為避免此情形發生，應關閉 Ping 功能的回應請求 | [edit system]<br>user@host#set<br>no-ping-record-route | 關閉 Ping 路由紀錄回應請求 | |
| 47 | TWGCB-03-002-0047 | | 關閉 Ping 的時間戳記回應請求 | 當 Ping 封包中包含時間戳記請求時，主機通常會以現在的系統時間回應，攻擊者可以透過這樣的方式，蒐集網路配置的資訊。為避免此情形發生， | [edit system]<br>user@host#set<br>no-ping-time-stamp | 關閉 Ping 時間戳記回應請 | |

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB設定值 | 備註 |
|---|---|---|---|---|---|---|---|
| | | | | 應關閉 Ping 功能的回應請求 | | 求 | |
| 48 | TWGCB-03-002-0048 | | 關閉 ICMP 的定向訊息 | 攻擊者可能利用 ICMP 重新定向功能獲取有關目標網絡的拓撲資訊，並加以識別利用。為了防止此情形，應在連接到不受信任的網絡(例如 Internet)的任何介面上禁用 ICMP 重定向訊息 | [edit system]<br>user@host#set no-redirects | 關閉 ICMP 定向訊息 | |
| 49 | TWGCB-03-002-0049 | | 限制以網路設備主機型號作為主機名稱 | 若以網路設備的型號、類型、製造商或是軟體版本等資訊作為主機的名稱，可能成為攻擊者資訊蒐集的內容，進一步危害網路設備的安全，為避免此情形發生，應限制以網路設備主機型號等資訊作為主機名稱 | [edit system]<br>user@host#set host-name <hostname> | 設置主機名稱 | |

資料來源：本中心整理

## 3. 參考文獻

[1]CIS Juniper JunOS Benchmark v1.0.1, https://benchmarks.cisecurity.org/tools2/CIS_Juniper_JunOS_Benchmark_v1.0.1.pdf