Fortinet SSLVPN 資安漏洞說明

JM Luo

02/10/2024

CVE-2024-21762 資安漏洞說明

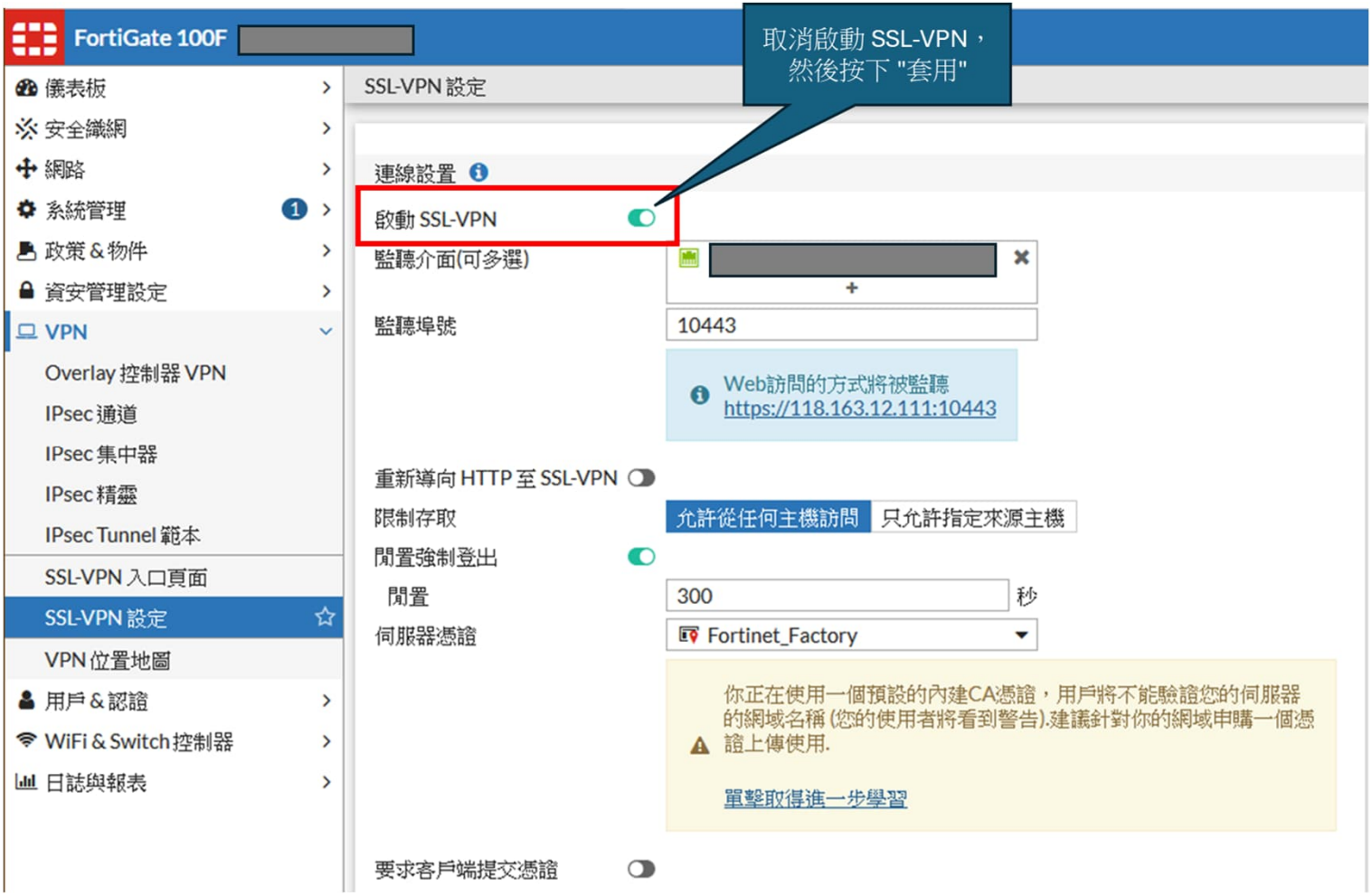
- CVE-2024-21762 為 FortiOS 上可能發生讓駭客利用 CWE-787 (A out-of-bounds write vulnerability) 可以藉由未經身份驗證的方式透過特製的 HTTP 請求執行任意程式碼或命令。
- 資安危險評分：9.6

- 資料來源網址：
  - Fortinet Warns of Critical FortiOS SSL VPN Flaw Likely Under Active Exploitation (thehackernews.com)
  - PSIRT | FortiGuard (fortinet.com)
  - Chinese Hackers Exploited FortiGate Flaw to Breach Dutch Military Network (thehackernews.com)

建議採取措施

- 取消 Fortinet SSLVPN 設定
  - 遠端管理暫時替代方式為使用 Anydesk 或 Teamviewer
- 升級到 Fortinet PSIRT 建議版本

取消 Fortinet SSLVPN 設定



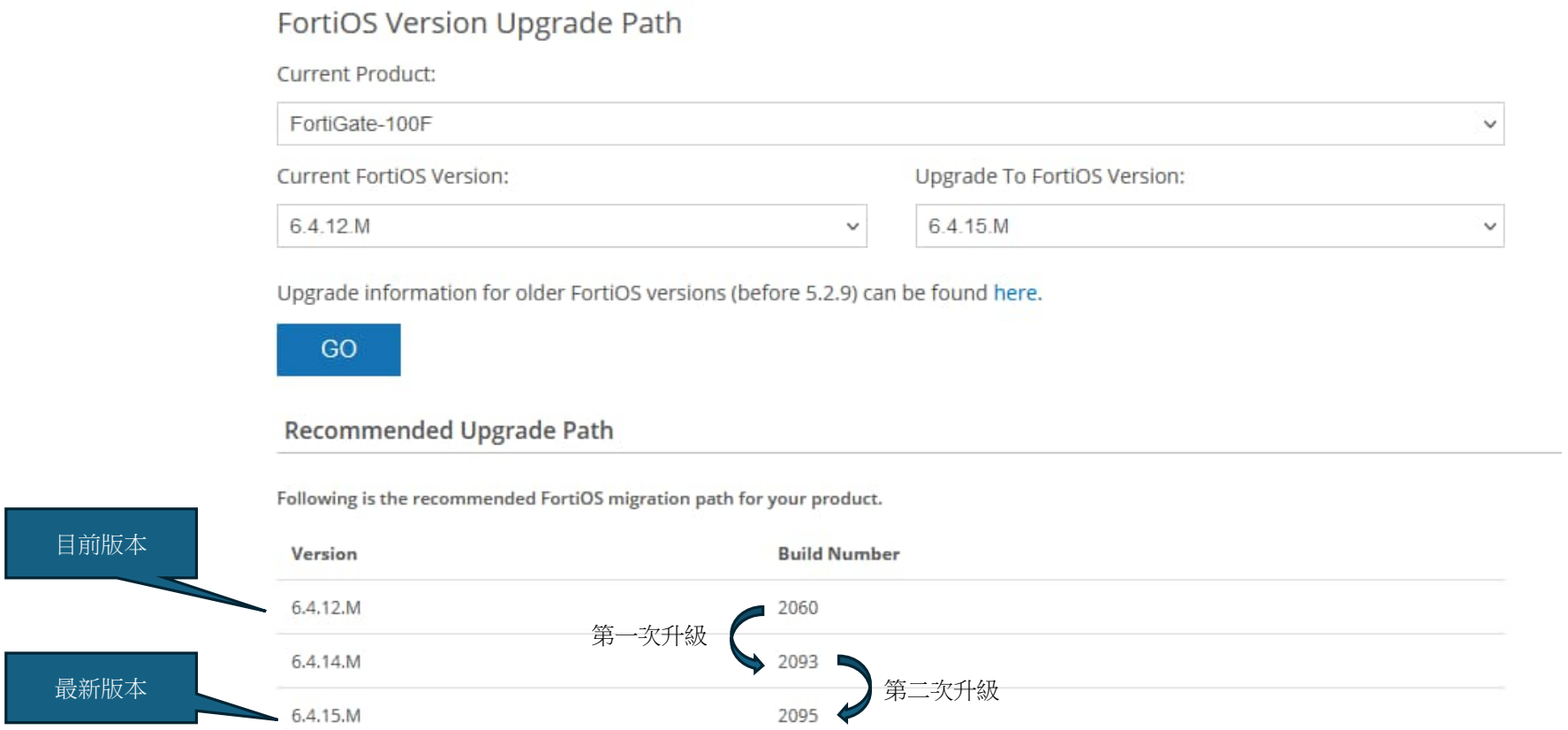
升級到 Fortinet PSIRT 建議版本

Version	Affected	Solution
FortiOS 7.6	Not affected	Not Applicable
FortiOS 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above
FortiOS 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above
FortiOS 7.0	7.0.0 through 7.0.13	Upgrade to 7.0.14 or above
FortiOS 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above
FortiOS 6.2	6.2.0 through 6.2.15	Upgrade to 6.2.16 or above
FortiOS 6.0	6.0 all versions	Migrate to a fixed release

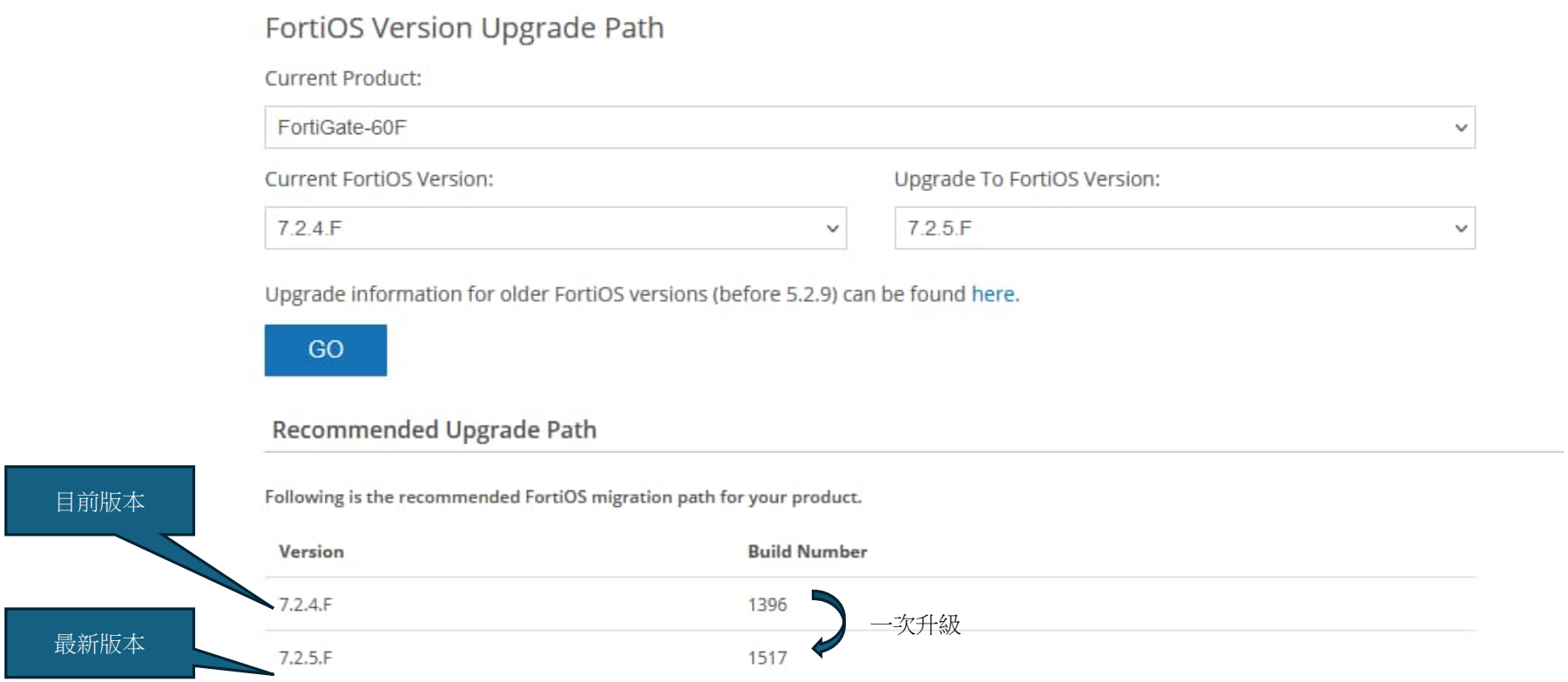
Follow the recommended upgrade path using our tool at: https://docs.fortinet.com/upgrade-tool

FortiSASE: Issue remediated Q1/24

Fortinet 6.4.x 版升級次序 (Upgrade Path)



Fortinet 7.2.x 版升級次序 (Upgrade Path)



Fortnet Firewall 單機升級方式

- 請登入 Fortinet Support 網站查詢升級步驟
  - https://support.fortinet.com/
- 依據目前版本升級到該版號的最新版本
  - 如 6.4.12 --> 6.4.14 --> 6.4.15
- 因單機升級會造成網路流量中斷，建議安排停機時間即發出公告
- 升級時間依機型不同而不同，每次升級約需 10 - 20 分鐘左右

Fortnet Firewall HA 架構升級步驟 - 1

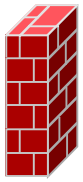
- 為避免在升級過程影響到使用者網路流量，請先使用 ssh 登入 Firewall，執行 "show full system ha"
- 檢查指令輸出，必須有 "set uninterruptible-upgrade enable" 此行設定
- 若沒有，請執行以下指令：
  - **config system ha**
    ```
        set uninterruptible-upgrade enable
    end
    ```

Fortnet Firewall HA 架構升級步驟 - 2

- 將昇級版本韌體上傳到目前的 Primary Firewall
- Primary Firewall 會將新版韌體推送給 Secondary Firewall
- Secondary Firewall 會開始進行版本升級並重啟，
- 當 Secondary Firewall 升級完成後，會向 Primary Firewall 發送已完成升級的確認訊息
- 當 Secondary Firewall 完成開機後會接手成為 Primary Firewall，原先的 Primary Firewall 會開始升級並重新啟動
- 當 Primary Firewall 再進行版本升級及重新啟動時，原先的 Secondary Firewall 會轉換身分為 Primary 身分，所有網路流量從先前的主節點轉移到新的主節點
- 升級過程完成後，系統會根據HA Override設定來確定新的 HA 架構誰是 Primary Firewall (主節點)，此功能預設為 Disable
- 因身分切換會造成流量瞬斷，建議升級完後保持當時狀態！

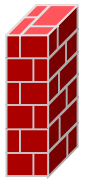
Fortnet Firewall HA 架構升級範例

Primary



1. 將新版 OS 上傳到 Primary

Secondary



2. Primary 將新版 OS 推送到 Secondary

3. Secondary 開始升級並重新啟動

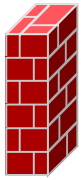
4. Primary 確認 Secondary 完成升級且開機完成

5. Secondary 完成開機後，成為 Primary

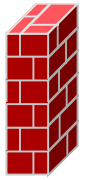
6. Primary 開始升級並重新啟動

7. Primary 啟動完成後，HA 架構依據設定保持當時身分

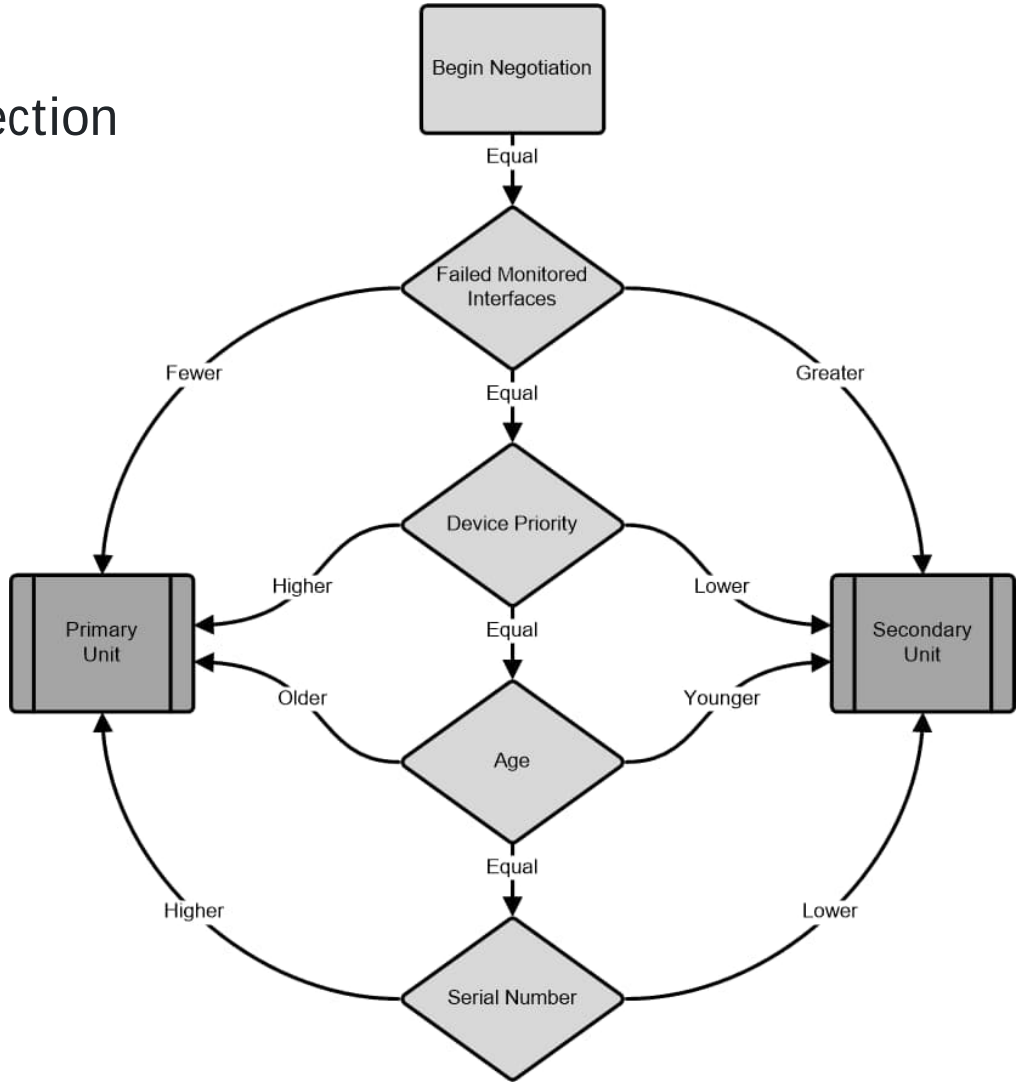
Secondary



Primary



Override and primary unit selection



遠端管理方式

- 在進行 Fortinet Firewall 升級前，請先完成可以從 Internet 使用如 Anydesk 、Teamviewer 、Google Chrome 之類的遠端管理設定，並做測試確認可以從外部連接到內部主機

SSL-VPN 其他替代方案

- WirGuard
  - https://www.wireguard.com/
  - https://www.asus.com/tw/support/faq/1048280/
- OpenVPN
  - https://openvpn.net/