步驟 3. 服務

未驗證用戶端的服務、使用不安全通訊協定的服務及使用太多權限執行的服務都有風險。如果不需要這些服務，請勿執行它們。藉由停用非必要服務，可以快速而輕易地減輕被攻擊的風險。也可以減輕維護 (補充程式、服務帳戶等) 的負擔。

如果要執行服務，請確定它是安全而持續的。若要如此，請使用最小權限帳戶執行該服務，並套用補充程式以維持在最近的狀態。

在此步驟中，您要：

- 停用非必要的服務。
- 停用 FTP、SMTP 及 NNTP，除非您需要它們。
- 停用 ASP.NET 狀態服務，除非您需要它們。

停用非必要的服務

Windows 服務容易受到可利用服務權限及功能並存取本機及遠端系統資源的攻擊者所傷害。防禦方法是停用系統及應用程式不需要的 Windows 服務。使用位於 [系統管理工具] 程式群組中的 [服務 MMC 嵌入式管理單元]，可以停用 Windows 服務。

注意 在停用服務之前，請確定先在測試或階移環境中測試其衝擊。

在多數狀態下，Web 伺服器不需要下列預設 Windows 服務：Alerter、Browser、Messenger、Netlogon (僅網域控制站有需要)、簡單 TCP/IP 服務及 Spooler。

Telnet 服務隨同 Windows 一起安裝，但預設並未啟用。IIS 系統管理員經常會啟用 Telnet。不過，它是不安全的通訊協定，容易受到利用。終端機服務提供比較安全的遠端系統管理選項。如需有關遠端系統管理的詳細資訊，請參閱本單元稍後的＜遠端系統管理＞。

停用 FTP、SMTP 及 NNTP，除非您需要它們

FTP、SMTP 及 NNTP 是容易被誤用的不安全通訊協定的範例。如果不需要這些服務，請勿執行它們。如果目前已在執行這些通訊協定，請嘗試尋找安全的替代方式。如果必須執行這些通訊協定，請保護其安全。

注意 IIS Lockdown 提供停用 FTP、SMTP 及 NNTP 的選項。

若要消除 FTP 利用的可能性，請在不使用時停用 FTP 服務。若是啟用 FTP 並可用於輸出連線，攻擊者就可以使用 FTP 從攻擊者的遠端系統上載檔案及工具到您的 Web 伺服器。一旦這些工具及檔案在您的 Web 伺服器上，攻擊者就可以攻擊 Web 伺服器或其他已連線的系統。

如果使用 FTP 通訊協定，用來存取 FTP 站台的使用者名稱及密碼與傳輸的資料都未經編碼或加密。IIS 不支援在 FTP 使用 SSL。如果安全通訊非常重要，而且您使用 FTP 做為傳輸通訊協定 (而不是 World Wide Web Distributed Authoring and Versioning (WebDAV) over SSL)，請考慮透過加密通道來使用 FTP。例如使用點對點通道通訊協定 (PPTP) 或網際網路通訊協定安全性 (IPSec) 來保護其安全的虛擬私人網路 (VPN)。

停用 ASP.NET 狀態服務，除非您需要它

.NET Framework 安裝 ASP.NET 狀態服務 (aspnet_state.exe)為 ASP.NET Web 應用程式及 Web 服務管理不在處理序中的使用者工作階段狀態。在預設狀態下，此服務設定為手動啟動，並以最小權限的本機 ASPNET 帳戶執行。如果沒有任何應用程式使用此服務來儲存狀態，請將它停用。如需有關保護 ASP.NET 工作階段狀態安全的詳細資訊，請參閱單元 19＜保護 ASP.NET 應用程式及 Web 服務的安全＞的＜工作階段狀態＞一節。

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/security:guideline:web_server_windows_step3

Last update: **2009/06/01 10:04**