張貼日期：2021/08/02

【資安漏洞預警】微軟Windows伺服器存在PetitPotam漏洞，請儘速確認並進行防護補強！

主旨：【資安漏洞預警】微軟Windows伺服器存在PetitPotam漏洞，允許攻擊者控制整個AD網域，請儘速確認並進行防護補強！

- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202107-1727□
  - 研究人員發現Windows伺服器存在PetitPotam漏洞，遠端攻擊者可利用遠端檔案系統加密(EFSRPC)協定強制AD伺服器向惡意伺服器執行NTLM身分驗證，並從中竊取資訊，進而控制整個AD網域。
- 影響平台:
  - Windows Server 2008 for 32-bit Systems Service Pack 2
  - Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
  - Windows Server 2008 for x64-based Systems Service Pack 2
  - Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
  - Windows Server 2008 R2 for x64-based Systems Service Pack 1
  - Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
  - Windows Server 2012 Windows Server 2012 (Server Core installation)
  - Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation)
  - Windows Server 2016 Windows Server 2016 (Server Core installation)
  - Windows Server 2019 Windows Server 2019 (Server Core installation)
  - Windows Server, version 2004 (Server Core installation)
  - Windows Server, version 20H2 (Server Core Installation)
- 建議措施:
  - 目前微軟官方已針對此漏洞釋出更新程式，請各機關聯絡設備維護廠商或參考以下網址儘速進行更新：
    - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36942
  - 若無法安裝更新程式請參考以下步驟採取緩解措施：
    1. 針對AD CS伺服器啟用身分驗證延伸保護措施(Extended Protection for Authentication, EPA)□並禁用HTTP□
    2. 開啟Internet Information Services (IIS)管理員→站台→CertSrv→驗證→Windows驗證→將選項設定為「需要」。
    3. 開啟Internet Information Services (IIS)管理員→站台→-CES_Kerberos→驗證→Windows驗證→將選項設定為「需要」。
    4. 在UI中啟用EPA後，CES建立之Web.config文件位於\systemdata\CES_CES_Kerberos\web.config□請於web.config檔中將設為Always□
    5. 開啟Internet Information Services (IIS)管理員→站台→CertSrv→SSL設定→勾選「需要SSL□□以限制僅能使用HTTPS連線。
    6. 重新啟動IIS□以使上述設定生效。

參考網址：https://msrc.microsoft.com/update-guide/vulnerability/ADV210003

- 參考資料:
  1. https://www.ithome.com.tw/news/145919
  2. https://msrc.microsoft.com/update-guide/vulnerability/ADV210003

3. https://support.microsoft.com/zh-tw/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429

計算機與通訊中心
網路系統組 敬啟