張貼日期：2022/02/10

【資安漏洞預警】特定版本Samba軟體存在高風險安全漏洞(CVE-2021-44142)允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新！

- 主旨說明：特定版本Samba軟體存在高風險安全漏洞(CVE-2021-44142)允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新！

- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-ANA-202202-0313
  - Samba是讓Unix/Linux作業系統與微軟Windows作業系統之間，透過SMB(Server Message Block)協定進行連結之軟體。研究人員發現Samba在預設組態(fruit:metadata=netatalk或fruit:resource=file)時，虛擬檔案系統(Virtual File System VFS)中之vfs_fruit模組在smbd開啟檔案與解析EA metadata過程中，存在越界記憶體堆積讀寫(out-of-bounds heap read/write)漏洞(CVE-2021-44142)導致攻擊者可以root權限執行任意程式碼。
- 影響平台:
  - Samba 4.13.17(不含)以前版本
- 建議措施:
  - Samba維護單位之官方網頁已針對此漏洞釋出更新程式，請各機關聯絡設備維護廠商進行版本確認並更新至4.13.17以上版本：https://www.samba.org/samba/security/
  - 若現階段無法立即更新Samba軟體之版本，則可開啟Samba組態檔(smb.conf)從VFS物件組態清單中移除fruit VFS模組，以減緩漏洞所造成之影響。
- 參考資料:
  - https://www.samba.org/samba/security/

計算機與通訊中心
網路系統組 敬啟