張貼日期：2026/02/10

【漏洞預警】CISA新增6個已知遭駭客利用之漏洞至KEV目錄(2026/02/02-2026/02/08)

- 主旨說明:【漏洞預警】CISA新增6個已知遭駭客利用之漏洞至KEV目錄(2026/02/02-2026/02/08)

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-200-202602-00000005
  - 【CVE-2021-39935】GitLab Community and Enterprise Editions Server-Side Request Forgery (SSRF) Vulnerability (CVSS v3.1: 6.8)
  - 【是否遭勒索軟體利用:未知】 GitLab Community 與 Enterprise 版本存在伺服器端請求偽造漏洞，可能允許未經授權的外部使用者透過 CI Lint API 執行伺服器端請求。
  - 【CVE-2025-64328】Sangoma FreePBX OS Command Injection Vulnerability (CVSS v3.1: 7.2)
  - 【是否遭勒索軟體利用:未知】 Sangoma FreePBX Endpoint Manager 存在作業系統指令注入漏洞，通過身分驗證的已知使用者可能透過 testconnection - check_ssh_connect() 函式進行指令注入，進而以 asterisk 使用者身分遠端存取系統。
  - 【CVE-2019-19006】Sangoma FreePBX Improper Authentication Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 Sangoma FreePBX 存在不當驗證漏洞，可能允許未經授權的使用者繞過密碼驗證機制，進而存取 FreePBX 管理介面所提供的服務。
  - 【CVE-2025-40551】SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 SolarWinds Web Help Desk 存在不受信任資料反序列化漏洞，可能導致遠端程式碼執行，使攻擊者能在主機上執行任意指令。
  - 【CVE-2025-11953】React Native Community CLI OS Command Injection Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 React Native Community CLI 存在作業系統指令注入漏洞，可能允許未經身分驗證的網路攻擊者向 Metro Development Server 發送 POST 請求，並透過伺服器暴露的易受攻擊端點執行任意可執行檔。在 Windows 環境中，攻擊者亦可執行具完全可控參數的任意 shell 指令。
  - 【CVE-2026-24423】SmarterTools SmarterMail Missing Authentication for Critical Function Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:是】 SmarterTools SmarterMail 的 ConnectToHub API 方法存在關鍵功能驗證缺失漏洞，可能允許攻擊者將 SmarterMail 執行個體指向惡意 HTTP 伺服器，可能導致執行惡意作業系統指令。
- 影響平台:
  - 【CVE-2021-39935】
  - 請參考官方所列的影響版本 https://about.gitlab.com/releases/2021/12/06/security-release-gitlab-14-5-2-released/
  - 【CVE-2025-64328】
  - 請參考官方所列的影響版本 https://github.com/FreePBX/security-reporting/security/advisories/GHSA-vm9p-46mv-5xvw
  - 【CVE-2019-19006】
  - FreePBX 13.0.0.0至13.0.197.13(含)版本
  - FreePBX 14.0.0.0至14.0.13.11(含)版本

    - FreePBX 15.0.0.0至15.0.16.26(含)版本
    - CVE-2025-40551
    - 請參考官方所列的影響版本 https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40551
    - CVE-2025-11953
    - 請參考官方所列的影響版本 https://github.com/advisories/GHSA-399j-vxmf-hjvr
    - CVE-2026-24423
    - SmarterMail Build 9511之前的版本
- 建議措施:
    - CVE-2021-39935 官方已針對漏洞釋出修復更新，請更新至相關版本 https://about.gitlab.com/releases/2021/12/06/security-release-gitlab-14-5-2-released/
    - CVE-2025-64328 官方已針對漏洞釋出修復更新，請更新至相關版本 https://github.com/FreePBX/security-reporting/security/advisories/GHSA-vm9p-46mv-5xvw
    - CVE-2019-19006 官方已針對漏洞釋出修復更新，請更新至相關版本 https://community.freepbx.org/t/freepbx-security-vulnerability-sec-2019-001/62772
    - CVE-2025-40551 官方已針對漏洞釋出修復更新，請更新至相關版本 https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40551
    - CVE-2025-11953 官方已針對漏洞釋出修復更新，請更新至相關版本 https://github.com/advisories/GHSA-399j-vxmf-hjvr
    - CVE-2026-24423 對應產品升級至以下版本(或更高) SmarterMail Build 9511

計算機與通訊中心
網路系統組 敬啟