張貼日期：2026/02/25

【漏洞預警】CISA新增8個已知遭駭客利用之漏洞至KEV目錄(2026/02/16-2026/02/22)

- 主旨說明:【漏洞預警】CISA新增8個已知遭駭客利用之漏洞至KEV目錄(2026/02/16-2026/02/22)

- 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-200-202602-00000010
  - 【CVE-2020-7796】Synacor Zimbra Collaboration Suite (ZCS) Server-Side Request Forgery Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 Synacor Zimbra Collaboration Suite (ZCS) 在安裝 WebEx zimlet 且啟用 zimlet JSP 的情況下存在伺服器端請求偽造漏洞。
  - 【CVE-2024-7694】TeamT5 ThreatSonar Anti-Ransomware Unrestricted Upload of File with Dangerous Type Vulnerability (CVSS v3.1: 7.2)
  - 【是否遭勒索軟體利用:未知】 TeamT5 ThreatSonar Anti-Ransomware產品上傳檔案內容過濾未臻完善，已取得產品平台管理權限之遠端攻擊者可上傳惡意檔案，並透過該檔案於伺服器上執行任意系統指令。
  - 【CVE-2008-0015】Microsoft Windows Video ActiveX Control Remote Code Execution Vulnerability (CVSS v3.1: 8.8)
  - 【是否遭勒索軟體利用:未知】 Microsoft Windows Video ActiveX 控制項存在遠端程式碼執行漏洞。攻擊者可透過製作特製的網頁來利用此漏洞。當使用者瀏覽該網頁時，可能導致遠端程式碼執行。成功利用此漏洞的攻擊者可能取得與已登入使用者相同的權限。
  - 【CVE-2026-2441】Google Chromium CSS Use-After-Free Vulnerability (CVSS v3.1: 8.8)
  - 【是否遭勒索軟體利用:未知】 Google Chromium CSS 存在使用釋放後記憶體漏洞，可能允許遠端攻擊者透過特製 HTML 頁面利用堆疊損毀。此漏洞可能影響多款使用 Chromium 的網頁瀏覽器，包括但不限於 Google Chrome、Microsoft Edge 及 Opera。
  - 【CVE-2021-22175】GitLab Server-Side Request Forgery (SSRF) Vulnerability (CVSS v3.1: 6.8)
  - 【是否遭勒索軟體利用:未知】 GitLab 在啟用對內部網路的 Webhook 請求時，存在伺服器端請求偽造漏洞。
  - 【CVE-2026-22769】Dell RecoverPoint for Virtual Machines (RP4VMs) Use of Hard-coded Credentials Vulnerability (CVSS v3.1: 10.0)
  - 【是否遭勒索軟體利用:未知】 Dell RecoverPoint for Virtual Machines (RP4VMs) 存在硬編碼憑證漏洞，可能允許未經驗證的遠端攻擊者取得底層作業系統存取權限，並維持持久存取。
  - 【CVE-2025-49113】RoundCube Webmail Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.9)
  - 【是否遭勒索軟體利用:未知】 RoundCube Webmail 存在反序列化不受信任資料漏洞，由於program/actions/settings/upload.php未能驗證 URL 中的 _from 參數，導致已驗證使用者可藉此漏洞遠端執行程式碼。
  - 【CVE-2025-68461】RoundCube Webmail Cross-site Scripting Vulnerability (CVSS v3.1: 7.2)
  - 【是否遭勒索軟體利用:未知】 RoundCube Webmail 存在跨站指令碼漏洞，攻擊者可透過 SVG 文件中的 animate 標籤加以利用。
- 影響平台:
  - 【CVE-2020-7796】請參考官方所列的影響版本 https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P7
  - 【CVE-2024-7694】ThreatSonar Anti-Ransomware 3.4.5(含)以前版本
  - 【CVE-2008-0015】請參考官方所列的影響版本

https://learn.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-037
    - CVE-2026-2441請參考官方所列的影響版本 https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_13.html
    - CVE-2021-22175請參考官方所列的影響版本 https://about.gitlab.com/releases/2021/02/11/security-release-gitlab-13-8-4-released/
    - CVE-2026-22769請參考官方所列的影響版本 https://www.dell.com/support/kbdoc/en-us/000426773/dsa-2026-079
    - CVE-2025-49113請參考官方所列的影響版本 https://roundcube.net/news/2025/06/01/security-updates-1.6.11-and-1.5.10
    - CVE-2025-68461請參考官方所列的影響版本 https://roundcube.net/news/2025/12/13/security-updates-1.6.12-and-1.5.12
- 建議措施:
    - CVE-2020-7796 官方已針對漏洞釋出修復更新，請更新至相關版本 https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P7
    - CVE-2024-7694 更新至3.5.0(含)以後版本，或利用 Hotfix-20240715 進行修補。
    - CVE-2008-0015 官方已針對漏洞釋出修復更新，請更新至相關版本 https://learn.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-037
    - CVE-2026-2441 官方已針對漏洞釋出修復更新，請更新至相關版本 https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_13.html
    - CVE-2021-22175 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/2021/02/11/security-release-gitlab-13-8-4-released/
    - CVE-2026-22769 官方已針對漏洞釋出修復更新，請更新至相關版本 https://www.dell.com/support/kbdoc/en-us/000426773/dsa-2026-079
    - CVE-2025-49113 官方已針對漏洞釋出修復更新，請更新至相關版本 https://roundcube.net/news/2025/06/01/security-updates-1.6.11-and-1.5.10
    - CVE-2025-68461 官方已針對漏洞釋出修復更新，請更新至相關版本 https://roundcube.net/news/2025/12/13/security-updates-1.6.12-and-1.5.12

計算機與通訊中心
網路系統組 敬啟