

## ANA事件單通知:TACERT-ANA-2026061601061818【漏洞預警】CISA新增7個已知遭駭客利用之漏洞至KEV目錄(2026/06/08-2026/06/14)

### 教育機構ANA通報平台

|      |                             |      |                     |
|------|-----------------------------|------|---------------------|
| 發佈編號 | TACERT-ANA-2026061601061818 | 發佈時間 | 2026-06-16 13:28:19 |
| 事故類型 | ANA-漏洞預警                    | 發現時間 | 2026-06-16 13:28:19 |
| 影響等級 | 低                           |      |                     |

[主旨說明:]【漏洞預警】CISA新增7個已知遭駭客利用之漏洞至KEV目錄(2026/06/08-2026/06/14)

[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-200-202606-00000011

#### 1. 【CVE-2026-42271】BerriAI LiteLLM Command Injection Vulnerability (CVSS v3.1: 8.8)

【是否遭勒索軟體利用:未知】 BerriAI LiteLLM 存在指令注入漏洞，可能導致任何已通過驗證的使用者（包括僅持有低權限內部使用者金鑰的使用者）在主機上執行任意指令。

【影響平台】請參考官方所列的影響版本

<https://github.com/BerriAI/litellm/security/advisories/GHSA-v4p8-mg3p-g94g>

#### 2. 【CVE-2026-50751】Check Point Security Gateway Improper Authentication Vulnerability (CVSS v3.1: 9.3)

【是否遭勒索軟體利用:已知】 Check Point Security Gateway 在 IKEv1 金鑰交換機制中存在不當驗證漏洞，可能導致未經驗證的遠端攻擊者繞過身分驗證機制，並在未持有有效使用者密碼的情況下建立遠端存取 VPN 連線。

【影響平台】請參考官方所列的影響版本

<https://support.checkpoint.com/results/sk/sk185033>

#### 3. 【CVE-2026-11645】Google Chromium V8 Out-of-Bounds Read and Write Vulnerability (CVSS v3.1: 8.8)

【是否遭勒索軟體利用:未知】 Google Chromium V8 存在越界讀取與寫入漏洞，遠端攻擊者可透過特製的 HTML 頁面，在沙箱內執行任意程式碼。此漏洞可能影響多款採用 Chromium 核心的網頁瀏覽器，包括但不限於 Google Chrome、Microsoft Edge 與 Opera。

【影響平台】請參考官方所列的影響版本

4. 【CVE-2026-7473】Arista Extensible Operating System Incomplete Comparison with Missing Factors Vulnerability (CVSS v3.1: 5.8)

【是否遭勒索軟體利用:未知】 Arista Extensible Operating System 存在Incomplete Comparison with Missing Factors漏洞。當交換器收到目的 IP 位址與其設定之解封裝 IP 相符的非預期通道封包時，可能錯誤地執行解封裝並予以轉送，進而導致未預期的流量處理行為。

【影響平台】請參考官方所列的影響版本

<https://www.arista.com/en/support/advisories-notice/security-advisory/24005-security-advisory-0137>

5. 【CVE-2026-20245】Cisco Catalyst SD-WAN Manager Improper Encoding or Escaping of Output Vulnerability (CVSS v3.1: 7.8)

【是否遭勒索軟體利用:未知】 Cisco Catalyst SD-WAN Manager存在Improper Encoding or Escaping of Output漏洞。此漏洞可能使已通過驗證的本機攻擊者，透過向受影響系統提供特製檔案，以 root 權限執行任意指令。

【影響平台】請參考官方所列的影響版本

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-4uxFrzx>  
【

6. CVE-2026-10520】Ivanti Sentry OS Command Injection Vulnerability (CVSS v3.1: 10.0)

【是否遭勒索軟體利用:未知】 Ivanti Sentry存在作業系統指令注入漏洞，可能使未經驗證的遠端使用者以 root 權限執行遠端程式碼。當 Sentry 設備處於未受管狀態，且其端點可從外部網路存取時，攻擊者可成功利用此漏洞。若搭配 EPMM 使用 mTLS，或透過 Neurons for MDM 限制 HTTPS 存取，即可使外部攻擊者無法存取相關介面。

【影響平台】請參考官方所列的影響版本

<https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Sentry-CVE-2026-10520-CVE-2026-10523>

7. 【CVE-2026-35273】Oracle PeopleSoft Enterprise PeopleTools Missing Authentication for Critical Function Vulnerability (CVSS v3.1: 9.8)

【是否遭勒索軟體利用:已知】 Oracle PeopleSoft Enterprise PeopleTools 存在關鍵功能缺乏身分鑑別漏洞。未經驗證的攻擊者可利用此漏洞取得 PeopleSoft Enterprise PeopleTools 的控制權。

【影響平台】請參考官方所列的影響版本 <https://www.oracle.com/security-alerts/alert-cve-2026-35273.html>

情資分享等級：WHITE (情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助轉發與通知轄下各單位知悉

[影響平台:]

詳細內容於內容說明欄之影響平台

[建議措施:]

1. 【CVE-2026-42271】 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://github.com/BerriAI/litellm/security/advisories/GHSA-v4p8-mg3p-g94g>

2. 【CVE-2026-50751】 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://support.checkpoint.com/results/sk/sk185033>

3. 【CVE-2026-11645】 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/2026/06/stable-channel-update-for-desktop\\_0153744567.html](https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html)

4. 【CVE-2026-7473】 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://www.arista.com/en/support/advisories-notice/security-advisory/24005-security-advisory-0137>

5. 【CVE-2026-20245】 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-4uxFrdzx>

6. 【CVE-2026-10520】 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Sentry-CVE-2026-10520-CVE-2026-10523>

7. 【CVE-2026-35273】 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://www.oracle.com/security-alerts/alert-cve-2026-35273.html>

[參考資料:]

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組

網址：<https://info.cert.tanet.edu.tw/>

專線電話：07-5250211

網路電話：98400000

E-Mail：[service@cert.tanet.edu.tw](mailto:service@cert.tanet.edu.tw)