張貼日期：2025/10/22

【漏洞預警】CISA新增6個已知遭駭客利用之漏洞至KEV目錄(2025/10/13-2025/10/19)

- 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(2025/10/13-2025/10/19)

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202510-00000011

1. 【CVE-2025-47827】IGEL OS Use of a Key Past its Expiration Date Vulnerability (CVSS v3.1: 4.6)
   - 【是否遭勒索軟體利用:未知】 IGEL OS存在安全功能繞過漏洞，由於 igel-flash-driver 模組未能正確驗證加密簽章，導致攻擊者可繞過安全啟動機制，並從未經驗證的 SquashFS 映像檔中掛載特製的根檔案系統。
   - 【影響平台】請參考官方所列的影響版本
   - https://kb.igel.com/en/security-safety/current/isn-2025-22-statement-on-cve-2025-47827-in-igel-os
2. 【CVE-2025-24990】Microsoft Windows Untrusted Pointer Dereference Vulnerability (CVSS v3.1: 7.8)
   - 【是否遭勒索軟體利用:未知】 Microsoft Windows Agere數據機驅動程式存在不可靠的指標反參考漏洞，可能導致權限提升。攻擊者若成功利用此漏洞，可能取得管理員權限。
   - 【影響平台】請參考官方所列的影響版本
   - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24990
3. 【CVE-2025-59230】Microsoft Windows Improper Access Control Vulnerability (CVSS v3.1: 7.8)
   - 【是否遭勒索軟體利用:未知】 Microsoft Windows的遠端存取連線管理員存在不當存取控制漏洞，可能允許未經授權的攻擊者在本機提升權限。
   - 【影響平台】請參考官方所列的影響版本
   - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59230
4. 【CVE-2025-6264】Rapid7 Velociraptor Incorrect Default Permissions Vulnerability (CVSS v3.1: 5.5)
   - 【是否遭勒索軟體利用:已知】 Rapid7 Velociraptor存在不正確的預設權限漏洞，可能導致任意指令執行及端點接管。要成功利用此漏洞，使用者必須具備COLLECT_CLIENT權限。
   - 【影響平台】請參考官方所列的影響版本
   - https://docs.velociraptor.app/announcements/advisories/cve-2025-6264/
5. 【CVE-2016-7836】SKYSEA Client View Improper Authentication Vulnerability (CVSS v3.1: 9.8)
   - 【是否遭勒索軟體利用:未知】 SKYSEA Client View 存在不當驗證漏洞，攻擊者可透過管理主控台程式與TCP連線時的驗證處理缺陷，實現遠端程式碼執行。
   - 【影響平台】請參考官方所列的影響版本
   - https://www.skygroup.jp/security-info/news/170308.html
6. 【CVE-2025-54253】Adobe Experience Manager Forms Code Execution Vulnerability (CVSS v3.1: 10.0)
   - 【是否遭勒索軟體利用:未知】 Adobe Experience Manager Forms in JEE存在未具體說明的漏洞，可能導致任意程式碼執行。
   - 【影響平台】請參考官方所列的影響版本
   - https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html

- 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-2025-47827 官方已針對漏洞釋出聲明，請更新至其他未受影響版本
     - https://kb.igel.com/en/security-safety/current/isn-2025-22-statement-on-cve-2025-47827-in-igel-os
  2. CVE-2025-24990 官方已針對漏洞釋出修復更新，請更新至相關版本
     - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24990
  3. CVE-2025-59230 官方已針對漏洞釋出修復更新，請更新至相關版本
     - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59230
  4. CVE-2025-6264 官方已針對漏洞釋出修復更新，請更新至相關版本
     - https://docs.velociraptor.app/announcements/advisories/cve-2025-6264/
  5. CVE-2016-7836 官方已針對漏洞釋出修復更新，請更新至相關版本
     - https://www.skygroup.jp/security-info/news/170308.html
  6. CVE-2025-54253 官方已針對漏洞釋出修復更新，請更新至相關版本
     - https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html

---

計算機與通訊中心
網路系統組 敬啟

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20251022_01

Last update: **2025/10/22 14:36**