張貼日期：2025/06/10

【漏洞預警】CISA新增9個已知遭駭客利用之漏洞至KEV目錄(2025/06/02-2025/06/08)

- 主旨說明:【漏洞預警】CISA新增9個已知遭駭客利用之漏洞至KEV目錄(2025/06/02-2025/06/08)

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202506-00000003

1. 【CVE-2021-32030】ASUS Routers Improper Authentication Vulnerability (CVSS v3.1: 9.8)
   - 【是否遭勒索軟體利用:未知】 ASUS Lyra Mini和ASUS GT-AC2900裝置存在不當驗證漏洞，攻擊者可未經授權存取管理介面。
   - 【影響平台】 ASUS GT-AC2900 3.0.04.386.42643之前的版本 ASUS Lyra Mini 3.0.0.4_384_46630之前的版本
2. 【CVE-2025-3935】ConnectWise ScreenConnect Improper Authentication Vulnerability (CVSS v3.1: 7.2)
   - 【是否遭勒索軟體利用:未知】 ConnectWise ScreenConnect存在不當驗證漏洞。此漏洞可能允許ViewState程式碼注入攻擊，若機器金鑰遭到洩漏，攻擊者可能藉此遠端執行任意程式碼。
   - 【影響平台】請參考官方所列的影響版本
   - https://www.connectwise.com/company/trust/security-bulletins/screenconnect-security-patch-2025.4
3. 【CVE-2025-35939】Craft CMS External Control of Assumed-Immutable Web Parameter Vulnerability (CVSS v3.1: 5.3)
   - 【是否遭勒索軟體利用:未知】 Craft CMS存在對可變網頁參數未充分驗證的漏洞。攻擊者可利用此漏洞，將任意內容(如PHP程式碼)寫入伺服器指定本機檔案路徑，可能導致遠端程式碼執行。
   - 【影響平台】 Craft CMS 4.15.3(不含)之前的版本 Craft CMS 5.00至5.7.5(不含)的版本
4. 【CVE-2024-56145】Craft CMS Code Injection Vulnerability (CVSS v3.1: 9.8)
   - 【是否遭勒索軟體利用:未知】 Craft CMS存在程式碼注入漏洞。若受影響版本的使用者在其php.ini設定中啟用了register_argc_argv則容易受到遠端程式碼執行的攻擊。
   - 【影響平台】請參考官方所列的影響版本
   - https://github.com/craftcms/cms/security/advisories/GHSA-2p6p-9rc9-62j9
5. 【CVE-2023-39780】ASUS RT-AX55 Routers OS Command Injection Vulnerability (CVSS v3.1: 8.8)
   - 【是否遭勒索軟體利用:未知】 ASUS RT-AX55裝置存在作業系統指令注入漏洞，遠端且已驗證的攻擊者可能藉此執行任意指令。
   - 【影響平台】 ASUS RT-AX55 3.0.0.4386.51598
6. 【CVE-2025-21479】Qualcomm Multiple Chipsets Incorrect Authorization Vulnerability (CVSS v3.1: 8.6)
   - 【是否遭勒索軟體利用:未知】 多款Qualcomm晶片組存在不當授權漏洞。此漏洞可在執行特定指令順序時，在GPU micronode執行未經授權的指令，導致記憶體損毀。
   - 【影響平台】請參考官方所列的影響版本
   - https://docs.qualcomm.com/product/publicresources/securitybulletin/june-2025-bulletin.html
7. 【CVE-2025-21480】Qualcomm Multiple Chipsets Incorrect Authorization Vulnerability (CVSS v3.1: 8.6)
   - 【是否遭勒索軟體利用:未知】 多款Qualcomm晶片組存在不當授權漏洞。此漏洞可在

執行特定指令順序時，在GPU micronode執行未經授權的指令，導致記憶體損毀。
    - 【影響平台】請參考官方所列的影響版本
    - https://docs.qualcomm.com/product/publicresources/securitybulletin/june-2025-bulletin.html
8. CVE-2025-27038Qualcomm Multiple Chipsets Use-After-Free Vulnerability (CVSS v3.1: 7.5)
    - 【是否遭勒索軟體利用:未知】 多款Qualcomm晶片組存在記憶體釋放後使用漏洞。此漏洞可在Chrome瀏覽器使用Adreno GPU驅動程式渲染圖形時造成記憶體損毀。
    - 【影響平台】請參考官方所列的影響版本
    - https://docs.qualcomm.com/product/publicresources/securitybulletin/june-2025-bulletin.html
9. CVE-2025-5419Google 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存在越界讀寫漏洞，遠端攻擊者可透過特製的HTML頁面，利用該漏洞進行堆積記憶體損毀攻擊。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 ChromeMicrosoft Edge和Opera
    - 【影響平台】請參考官方所列的影響版本
    - https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop.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-2021-32030 受影響的產品可能已達到生命週期終止(EoL)或服務終止(EoS)建議使用者停止使用相關產品。
2. CVE-2025-3935 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://www.connectwise.com/company/trust/security-bulletins/screenconnect-security-patch-2025.4
3. CVE-2025-35939 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://github.com/craftcms/cms/releases/tag/4.15.3
    - https://github.com/craftcms/cms/releases/tag/5.7.5
4. CVE-2024-56145 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://github.com/craftcms/cms/security/advisories/GHSA-2p6p-9rc9-62j9
5. CVE-2023-39780 對應產品升級至以下版本(或更高) ASUS RT-AX55 3.0.0.4.386_53119
6. CVE-2025-21479 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://docs.qualcomm.com/product/publicresources/securitybulletin/june-2025-bulletin.html
7. CVE-2025-21480 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://docs.qualcomm.com/product/publicresources/securitybulletin/june-2025-bulletin.html
8. CVE-2025-27038 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://docs.qualcomm.com/product/publicresources/securitybulletin/june-2025-bulletin.html
9. CVE-2025-5419 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/2025/06/stable-channel-update-for-desktop.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:20250610_02

Last update: **2025/06/10 14:14**