張貼日期：2025/10/14

【漏洞預警】CISA新增9個已知遭駭客利用之漏洞至KEV目錄(2025/10/06-2025/10/12)

- 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(2025/10/06-2025/10/12)

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202510-00000004

1. 【CVE-2021-22555】Linux Kernel Heap Out-of-Bounds Write Vulnerability (CVSS v3.1: 8.3)
   - 【是否遭勒索軟體利用:未知】 Linux核心存在堆積越界寫入漏洞，攻擊者可利用該漏洞透過使用者命名空間提升權限或造成DoS(透過堆積記憶體損毀方式)。
   - 【影響平台】 Linux Kernel 2.6.19-rc1(含)之後的版本
2. 【CVE-2010-3962】Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (CVSS v3.1: 8.1)
   - 【是否遭勒索軟體利用:未知】 Microsoft Internet Explorer存在未初始化記憶體損毀漏洞，可能允許遠端程式碼執行。
   - 【影響平台】請參考官方所列的影響版本
   - https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-090
3. 【CVE-2021-43226】Microsoft Windows Privilege Escalation Vulnerability (CVSS v3.1: 7.8)
   - 【是否遭勒索軟體利用:已知】 Microsoft Windows 通用日誌檔案系統驅動程式存在權限提升漏洞，可能允許具備本地特權的攻擊者繞過特定安全機制。
   - 【影響平台】請參考官方所列的影響版本
   - https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-43226
4. 【CVE-2013-3918】Microsoft Windows Out-of-Bounds Write Vulnerability (CVSS v3.1: 8.8)
   - 【是否遭勒索軟體利用:未知】 Microsoft Windows在InformationCardSigninHelper類別的ActiveX控制項 (icardie.dll) 存在越界寫入漏洞。攻擊者可透過特製的網頁來利用此漏洞。當使用者瀏覽該網頁時，此漏洞可能導致遠端程式碼執行。成功利用此漏洞的攻擊者可取得與當前使用者相同的權限。受影響的產品可能已達生命週期終止(EoL)或停止服務(EoS)，建議使用者停止使用該產品。
   - 【影響平台】請參考官方所列的影響版本
   - https://learn.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-090
5. 【CVE-2011-3402】Microsoft Windows Remote Code Execution Vulnerability (CVSS v3.1: 8.8)
   - 【是否遭勒索軟體利用:未知】 Microsoft Windows Kernel在核心模式驅動程式win32k.sys中的TrueType字型解析引擎存在漏洞，可能允許遠端攻擊者透過特製的字型資料，在Word文件或網頁中執行任意程式碼。
   - 【影響平台】請參考官方所列的影響版本
   - https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2011/ms11-087
6. 【CVE-2010-3765】Mozilla Multiple Products Remote Code Execution Vulnerability (CVSS v3.1: 9.8)
   - 【是否遭勒索軟體利用:未知】 Mozilla Firefox、SeaMonkey與Thunderbird在啟用JavaScript時存在未具體說明的漏洞。遠端攻擊者可透過與 nsCSSFrameConstructor::ContentAppended、appendChild 方法、不正確的索引追蹤，及建立多個框架等相關的攻擊向量，導致記憶體損毀，進而執行任意程式碼。
   - 【影響平台】請參考官方所列的影響版本
   - https://blog.mozilla.org/security/2010/10/26/critical-vulnerability-in-firefox-3-5-and-firefox-3-6/

7. CVE-2025-61882Oracle E-Business Suite Unspecified Vulnerability (CVSS v3.1: 9.8)
   - 【是否遭勒索軟體利用:是】Oracle E-Business Suite 的 BI Publisher 整合元件存在未具體說明的漏洞，可能允許透過 HTTP 且未經驗證的攻擊者入侵並接管 Oracle Concurrent Processing。
   - 【影響平台】請參考官方所列的影響版本
   - https://www.oracle.com/security-alerts/alert-cve-2025-61882.html
8. CVE-2025-27915Synacor Zimbra Collaboration Suite (ZCS) Cross-site Scripting Vulnerability (CVSS v3.1: 5.4)
   - 【是否遭勒索軟體利用:未知】Synacor Zimbra Collaboration Suite(ZCS)的經典 Web 用戶端存在跨站指令碼（XSS）漏洞，起因於系統對 ICS 檔案中 HTML 內容的過濾不足。當使用者檢視含有惡意 ICS 項目的電子郵件時，內嵌的 JavaScript 會透過標籤內的 ontoggle 事件被執行。攻擊者可藉此在受害者的工作階段中執行任意 JavaScript 程式碼，進而執行未經授權的操作，例如設定郵件篩選器以將郵件轉寄至攻擊者控制的地址。最終，攻擊者可能對受害者帳戶執行未經授權的操作，進行郵件轉寄或資料外洩等行為。
   - 【影響平台】請參考官方所列的影響版本
   - https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories
9. CVE-2021-43798Grafana Path Traversal Vulnerability (CVSS v3.1: 7.5)
   - 【是否遭勒索軟體利用:未知】Grafana存在路徑遍歷漏洞，可能允許攻擊者存取本機檔案。
   - 【影響平台】請參考官方所列的影響版本
   - https://github.com/grafana/grafana/security/advisories/GHSA-8pjx-jj86-j47p

- 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-2021-22555 官方已針對漏洞釋出修復更新，請更新至相關版本
     - (1). https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/net/netfilter/x_tables.c?id=9fa492cdc160cd27ce1046cb36f47d3b2b1efa21
     - (2). https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/net/netfilter/x_tables.c?id=b29c457a6511435960115c0f548c4360d5f4801d
  2. CVE-2010-3962 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/2010/ms10-090
  3. CVE-2021-43226 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/en-US/advisory/CVE-2021-43226
  4. CVE-2013-3918 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/2013/ms13-090
  5. CVE-2011-3402 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/2011/ms11-087
  6. CVE-2010-3765 官方已針對漏洞釋出修復更新，請更新至相關版本
     - https://blog.mozilla.org/security/2010/10/26/critical-vulnerability-in-firefox-3-5-and-firefox-3-6/
  7. CVE-2025-61882 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-2025-61882.html
  8. CVE-2025-27915 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_Security_Advisories
  9. CVE-2021-43798 官方已針對漏洞釋出修復更新，請更新至相關版本
     - https://github.com/grafana/grafana/security/advisories/GHSA-8pjx-jj86-j47p

---

計算機與通訊中心

網路系統組 敬啟