張貼日期：2026/09/16

【漏洞預警】CISA新增11個已知遭駭客利用之漏洞至KEV目錄(2026/08/24-2026/08/30)

- 主旨說明:【漏洞預警】CISA新增11個已知遭駭客利用之漏洞至KEV目錄(2026/08/24-2026/08/30)

- 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-200-202609-00000008
  - 【CVE-2026-21962】Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in Improper Access Control Vulnerability (CVSS v3.1: 10.0)
  - 【是否遭勒索軟體利用:未知】 Oracle HTTP Server及Oracle WebLogic Server Proxy Plug-in存在不當存取控制漏洞，可能導致未經授權的使用者取得對關鍵資料的建立、刪除或修改權限，以及未經授權存取關鍵資料，甚至可能完全存取Oracle HTTP Server及Oracle WebLogic Server Proxy Plug-in所能存取的所有資料。
  - 【CVE-2026-60004】Gitea Code Injection Vulnerability (CVSS v31: 9.8)
  - 【是否遭勒索軟體利用:未知】 Gitea存在程式碼注入漏洞，具備儲存庫寫入權限的攻擊者可向diffpatch API端點傳送惡意修補程式，以植入可執行的Git hook【並以Gitea服務帳戶的身分執行Shell指令。
  - 【CVE-2021-23758】Ajax.NET Professional Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 8.1)
  - 【是否遭勒索軟體利用:未知】 Ajax.NET Professional【AjaxPro】存在反序列化不受信任資料漏洞，可能允許攻擊者利用任意 .NET 類別執行遠端程式碼。受影響的產品可能已達產品生命週期終止【EoL】及／或服務終止【EoS】】建議使用者停止使用受影響產品，並／或轉移至受支援的版本。
  - 【CVE-2015-3246】Red Hat Libuser Race Condition Vulnerability (CVSS v3.1: 5.1)
  - 【是否遭勒索軟體利用:未知】 Red Hat libuser存在條件競爭漏洞，允許已通過身分驗證的本機使用者損毀 /etc/passwd 檔案，進而導致阻斷服務或權限提升。
  - 【CVE-2015-5287】Red Hat Automatic Bug Reporting Tool Privilege Escalation Vulnerability (CVSS v3.1: 7.8)
  - 【是否遭勒索軟體利用:未知】 Red Hat Automatic Bug Reporting Tool【ABRT】存在權限提升漏洞，可能使具備特定權限的本機使用者透過針對名稱可預測的檔案發動符號連結攻擊，取得更高權限。受影響的產品可能已達產品生命週期終止【EoL】及／或服務終止【EoS】】建議使用者停止使用受影響產品，並／或轉移至受支援的版本。
  - 【CVE-2022-0995】Linux Kernel Out-of-Bounds Write Vulnerability (CVSS v3.1: 7.8)
  - 【是否遭勒索軟體利用:未知】 Linux Kernel 存在越界寫入漏洞，可能使本機使用者取得特權存取權限，或導致系統發生阻斷服務。
  - 【CVE-2026-8452】Citrix NetScaler ADC and NetScaler Gateway Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 Citrix NetScaler ADC 及 NetScaler Gateway 存在記憶體緩衝區邊界內操作限制不當漏洞，可能導致阻斷服務。
  - 【CVE-2019-1068】Microsoft SQL Server Remote Code Execution Vulnerability (CVSS v3.1: 8.8)
  - 【是否遭勒索軟體利用:未知】 Microsoft SQL Server存在遠端程式碼執行漏洞，可能使攻擊者以SQL Server Database Engine服務帳戶的身分執行程式碼。
  - 【CVE-2023-49105】ownCloud Improper Authentication Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知】 ownCloud 存在不當驗證漏洞，若攻擊者已知受害者的使用者名稱，且該受害者未設定簽署金鑰，攻擊者即可在未經驗證的情況下存取、修改或刪除任何檔

案。
    - CVE-2026-53362Linux Kernel Unspecified Vulnerability (CVSS v3.1: 7.8)
    - 【是否遭勒索軟體利用:未知】 Linux Kernel 存在未具體說明的漏洞，可能使攻擊者透過 IPv6 網路子系統進行權限提升。此漏洞可能影響多項產品，包括但不限於 SuseRed Hat 及其他使用 Linux 的產品。
    - CVE-2026-66384JFrog Artifactory Improper Limitation of a Pathname to a Restricted Directory Vulnerability (CVSS v3.1: 5.3)
    - 【是否遭勒索軟體利用:未知】 JFrog Artifactory 存在路徑名稱不當限制於受限目錄的漏洞。在特定遠端儲存庫條件下，此漏洞可能允許已通過身分驗證的使用者，將資料寫入預期的 Docker 快取路徑以外的位置。
- 影響平台:
    - CVE-2026-21962請參考官方所列的影響版本 https://www.oracle.com/security-alerts/cpujan2026.html
    - CVE-2026-60004請參考官方所列的影響版本 https://github.com/go-gitea/gitea/security/advisories/GHSA-rcr6-4jqh-j84m
    - CVE-2021-23758請參考官方所列的影響版本 https://github.com/michaelschwarz/Ajax.NET-Professional/commit/b0e63be5f0bb20dfce507cb8a1a9568f6e73de57
    - CVE-2015-3246請參考官方所列的影響版本 https://access.redhat.com/articles/1537873
    - CVE-2015-5287請參考官方所列的影響版本 https://access.redhat.com/errata/RHSA-2015:2505.html
    - CVE-2022-0995請參考官方所列的影響版本 https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=93ce93587d36493f2f86921fa79921b3cba63fbb
    - CVE-2026-8452請參考官方所列的影響版本 https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604
    - CVE-2019-1068請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-1068
    - CVE-2023-49105請參考官方所列的影響版本 https://owncloud.com/security-advisories/webdav-api-authentication-bypass-using-pre-signed-urls/
    - CVE-2026-53362請參考官方所列的影響版本 https://lore.kernel.org/linux-cve-announce/2026070450-CVE-2026-53362-fe9b@gregkh/T/#u
    - CVE-2026-66384請參考官方所列的影響版本 https://docs.jfrog.com/releases/docs/jfrog-security-advisories
- 建議措施:
    - CVE-2026-21962 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/cpujan2026.html
    - CVE-2026-60004 官方已針對漏洞釋出修復更新，請更新至相關版本 https://github.com/go-gitea/gitea/security/advisories/GHSA-rcr6-4jqh-j84m
    - CVE-2021-23758 官方已針對漏洞釋出修復更新，請更新至相關版本 https://github.com/michaelschwarz/Ajax.NET-Professional/commit/b0e63be5f0bb20dfce507cb8a1a9568f6e73de57
    - CVE-2015-3246 官方已針對漏洞釋出修復更新，請更新至相關版本 https://access.redhat.com/articles/1537873
    - CVE-2015-5287 官方已針對漏洞釋出修復更新，請更新至相關版本 https://access.redhat.com/errata/RHSA-2015:2505.html
    - CVE-2022-0995 官方已針對漏洞釋出修復更新，請更新至相關版本 https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=93ce93587d36493f2f86921fa79921b3cba63fbb

  - 【CVE-2026-8452】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604
  - 【CVE-2019-1068】 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-2019-1068
  - 【CVE-2023-49105】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://owncloud.com/security-advisories/webdav-api-authentication-bypass-using-pre-signed-urls/
  - 【CVE-2026-53362】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://lore.kernel.org/linux-cve-announce/2026070450-CVE-2026-53362-fe9b@gregkh/T/#u
  - 【CVE-2026-66384】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://docs.jfrog.com/releases/docs/jfrog-security-advisories
- 參考資料:

計算機與通訊中心
網路系統組 敬啟