張貼日期：2025/12/29

【漏洞預警】CISA新增7個已知遭駭客利用之漏洞至KEV目錄(2025/12/15-2025/12/21)

- 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(2025/12/15-2025/12/21)/ *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-200-202512-00000011 * 【CVE-2025-14611】Gladinet CentreStack and Triofox Hard Coded Cryptographic Vulnerability (CVSS v3.1: 9.8) * 【是否遭勒索軟體利用:未知】 Gladinet CentreStack 與TrioFox 因其 AES 加密方案的實作方式，存在硬編碼加密金鑰漏洞。*此漏洞會降低對外公開端點的安全性，若未經驗證即接收特製的請求，可能會受任意本地檔案包含影響】 * 【CVE-2025-43529】Apple Multiple Products Use-After-Free WebKit Vulnerability (CVSS v3.1: 8.8) * 【是否遭勒索軟體利用:未知】 Apple iOS、iPadOS、macOS 及其他 Apple 產品中的 WebKit 存在記憶體釋放後使用漏洞。在處理惡意設計的網頁內容時，可能導致記憶體損毀。*此漏洞可能影響所有使用 WebKit 的HTML 解析器，包括但不限於 Apple Safari以及其他依賴 WebKit 進行 HTML 處理的非 Apple 產品】 * 【CVE-2025-59718】Fortinet Multiple Products Improper Verification of Cryptographic Signature Vulnerability (CVSS v3.1: 9.8) * 【是否遭勒索軟體利用:未知】 Fortinet FortiOS、FortiSwitchMaster、FortiProxy 與FortiWeb 存在加密簽章驗證不當漏洞。*此漏洞可能允許未經身分驗證的攻擊者，透過特製的 SAML 訊息繞過 FortiCloud SSO 登入驗證。請注意【CVE-2025-59719 涉及相同問題，並已於同份廠商公告中提及。請務必套用該公告中所列的所有修補程式】 * 【CVE-2025-59374】ASUS Live Update Embedded Malicious Code Vulnerability (CVSS v3.1: 9.8) * 【是否遭勒索軟體利用:未知】 ASUS Live Update 含有嵌入式惡意程式碼漏洞，該客戶端曾因供應鏈遭入侵而在未經授權情況下修改後發行。*經修改的版本可能導致符合特定目標條件的裝置執行非預期的行為。受影響的產品可能已達生命週期終止【EoL】及／或服務終止【EoS】【建議使用者立即停止使用該產品】 * 【CVE-2025-40602】SonicWall SMA1000 Missing Authorization Vulnerability (CVSS v3.1: 6.6) * 【是否遭勒索軟體利用:未知】 SonicWall SMA1000 存在授權缺失漏洞，可能導致受影響裝置的設備管理控制台 (AMC) 發生權限提升】 * 【CVE-2025-20393】Cisco Multiple Products Improper Input Validation Vulnerability (CVSS v3.1: 10.0) * 【是否遭勒索軟體利用:未知】 Cisco Secure Email Gateway、Secure Email、AsyncOS 軟體以及 Web Manager 設備中存在輸入驗證不當漏洞，該漏洞可能允許威脅行為者在受影響設備的底層作業系統上，以 root 權限執行任意指令】 * 【CVE-2025-14733】WatchGuard Firebox Out of Bounds Write Vulnerability (CVSS v3.1: 9.8) * 【是否遭勒索軟體利用:未知】 WatchGuard Fireware OS 的iked 程序存在越界寫入漏洞。*此漏洞可能允許未經身分驗證的遠端攻擊者執行任意程式碼，並影響使用 IKEv2 的行動用戶 VPN 以及配置了動態閘道對等體的使用 IKEv2 的分公司 VPN】 * 影響平台: * 【CVE-2025-14611】 Gladinat CentreStack 16.12.10420.56791(不含)之前的版本 Gladinat Triofox 16.12.10420.56791(不含)之前的版本 * 【CVE-2025-43529】請參考官方所列的影響版本 https://support.apple.com/en-us/125884 * https://support.apple.com/en-us/125885 * https://support.apple.com/en-us/125886 * https://support.apple.com/en-us/125889 * https://support.apple.com/en-us/125890 * https://support.apple.com/en-us/125891 * https://support.apple.com/en-us/125892 * 【CVE-2025-59718】請參考官方所列的影響版本 https://fortiguard.fortinet.com/psirt/FG-IR-25-647 * 【CVE-2025-59374】請參考官方所列的影響版本 https://www.asus.com/news/hqfgvuyz6uyayje1/ * 【CVE-2025-40602】請參考官方所列的影響版本 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0019 * 【CVE-2025-20393】請參考官方所列的影響版本 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4 * 【CVE-2025-14733】請參考官方所列的影響版本 https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00027 *建議措施:* 【CVE-2025-14611】 對應產品升級至以下版本(或更高) Gladinat CentreStack 16.12.10420.56791 Gladinat Triofox 16.12.10420.56791 * 【CVE-2025-43529】 官方已針對漏洞釋出修復更新，請更新

*至相關版本 *https://support.apple.com/en-us/125884 * https://support.apple.com/en-us/125885 * https://support.apple.com/en-us/125886 * https://support.apple.com/en-us/125889 * https://support.apple.com/en-us/125890 * https://support.apple.com/en-us/125891 * https://support.apple.com/en-us/125892 * CVE-2025-59718 官方已針對漏洞釋出修復更新，請更新至相關版本 https://fortiguard.fortinet.com/psirt/FG-IR-25-647 * CVE-2025-59374 官方已針對漏洞釋出修復更新，請更新至相關版本 https://www.asus.com/news/hqfgvuyz6uyayje1/ * CVE-2025-40602 官方已針對漏洞釋出修復更新，請更新至相關版本 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0019 * CVE-2025-20393 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-sma-attack-N9bf4 * CVE-2025-14733 官方已針對漏洞釋出修復更新，請更新至相關版本 https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00027 —- 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:20251229_04

Last update: **2025/12/29 11:24**