張貼日期：2025/06/19

【漏洞預警】CISA新增4個已知遭駭客利用之漏洞至KEV目錄(2025/06/09-2025/06/15)

- 主旨說明:【漏洞預警】CISA新增4個已知遭駭客利用之漏洞至KEV目錄(2025/06/09-2025/06/15)

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202506-00000011
  1. 【CVE-2024-42009】RoundCube Webmail Cross-Site Scripting Vulnerability (CVSS v3.1: 9.3)
     - 【是否遭勒索軟體利用:未知】 RoundCube Webmail存在跨網站指令碼漏洞，可能允許遠端攻擊者利用program/actions/mail/show.php中message_body()函式的資料反清洗問題，透過特製的電子郵件竊取及傳送受害者的電子郵件。
     - 【影響平台】請參考官方所列的影響版本
     - https://roundcube.net/news/2024/08/04/security-updates-1.6.8-and-1.5.8
  2. 【CVE-2025-32433】Erlang Erlang/OTP SSH Server Missing Authentication for Critical Function Vulnerability (CVSS v3.1: 10.0)
     - 【是否遭勒索軟體利用:未知】 Erlang/OTP SSH伺服器存在關鍵功能驗證缺失漏洞。該漏洞可能允許攻擊者在未提供有效憑證的情況下執行任意指令，進而導致未經驗證的遠端程式碼執行。惡意使用者可利用SSH通訊協定訊息處理方式的漏洞，未經授權存取受影響的系統。此漏洞可能影響多種使用Erlang/OTP SSH伺服器的產品，包括但不限於Cisco、NetApp和SUSE。
     - 【影響平台】請參考官方所列的影響版本
     - https://github.com/erlang/otp/security/advisories/GHSA-37cp-fgq5-7wc2
  3. 【CVE-2025-33053】Web Distributed Authoring and Versioning (WebDAV) External Control of File Name or Path Vulnerability (CVSS v3.1: 8.8)
     - 【是否遭勒索軟體利用:未知】 WebDAV存在檔案名稱或路徑的外部控制漏洞。該漏洞可能允許未經授權的攻擊者透過網路遠端執行程式碼。此漏洞可能影響多種實作WebDAV的產品，包括但不限於Microsoft Windows。
     - 【影響平台】請參考官方所列的影響版本
     - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33053
  4. 【CVE-2025-24016】Wazuh Server Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.9)
     - 【是否遭勒索軟體利用:未知】 Wazuh存在不受信任資料的反序列化漏洞，該漏洞可導致在Wazuh伺服器上執行遠端程式碼。
     - 【影響平台】請參考官方所列的影響版本
     - https://github.com/wazuh/wazuh/security/advisories/GHSA-hcrc-79hj-m3qh
- 影響平台:
  - 詳細內容於內容說明欄之影響平台

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:20250619_01

Last update: **2025/06/19 13:34**