張貼日期：2025/10/01

【漏洞預警】CISA新增3個已知遭駭客利用之漏洞至KEV目錄(2025/09/22-2025/09/28)

- 主旨說明:【漏洞預警】CISA新增3個已知遭駭客利用之漏洞至KEV目錄(2025/09/22-2025/09/28)

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202510-00000001
  1. 【CVE-2025-10585】Google Chromium V8 Type Confusion Vulnerability (CVSS v3.1: 9.8)
     - 【是否遭勒索軟體利用:未知】 Google Chromium在其V8 JavaScript與WebAssembly引擎中存在類型混淆漏洞，遠端攻擊者可利用此漏洞達到遠端執行任意程式碼或造成程式崩潰。
     - 【影響平台】請參考官方所列的影響版本
     - https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_17.html
  2. 【CVE-2025-20362】Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Missing Authorization Vulnerability (CVSS v3.1: 6.5)
     - 【是否遭勒索軟體利用:未知】 Cisco安全防火牆自適應安全設備(ASA)和安全防火牆威脅防禦(FTD)的VPN Web伺服器中存在授權缺失漏洞。此漏洞可能與CVE-2025-20333串聯利用。
     - 【影響平台】請參考官方所列的影響版本
     - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-YROOTUW
  3. 【CVE-2025-20333】Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Buffer Overflow Vulnerability (CVSS v3.1: 9.9)
     - 【是否遭勒索軟體利用:未知】 Cisco安全防火牆自適應安全設備(ASA)和安全防火牆威脅防禦(FTD)的VPN Web伺服器中存在緩衝區溢位漏洞，可能導致遠端執行程式碼。此漏洞可能與CVE-2025-20362串聯利用。
     - 【影響平台】請參考官方所列的影響版本
     - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB
- 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-2025-10585】 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/2025/09/stable-channel-update-for-desktop_17.html
  2. 【CVE-2025-20362】 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-asaftd-webvpn-YROOTUW
  3. 【CVE-2025-20333】 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-asaftd-webvpn-z5xP8EUB

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:20251001_02

Last update: **2025/10/01 16:14**