張貼日期：2026/07/24

【漏洞預警□CISA新增10個已知遭駭客利用之漏洞至KEV目錄(2026/07/13-2026/07/19)

- 主旨說明:【漏洞預警□CISA新增10個已知遭駭客利用之漏洞至KEV目錄(2026/07/13-2026/07/19)

- 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-200-202607-00000011
  - □CVE-2008-4128□Cisco IOS Cross-Site Request Forgery Vulnerability (CVSS v3.1: 4.3)
  - 【是否遭勒索軟體利用:未知□ Cisco 871 Integrated Services Router 所使用的 Cisco IOS 12.4□其 HTTP Administration 元件存在多個跨網站請求偽造漏洞。遠端攻擊者可能誘使使用者發送特製請求，進而在受影響裝置上執行任意指令。
  - □CVE-2026-56155□Microsoft Active Directory Federation Services Insufficient Granularity of Access Control Vulnerability (CVSS v3.1: 7.8)
  - 【是否遭勒索軟體利用:未知□ Microsoft Active Directory Federation Services 存在存取控制粒度不足漏洞，允許經授權的攻擊者在本機提升權限。
  - □CVE-2026-56164□Microsoft SharePoint Server Missing Authentication for Critical Function Vulnerability (CVSS v3.1: 5.3)
  - 【是否遭勒索軟體利用:未知□ Microsoft SharePoint Server存在關鍵功能缺乏身分鑑別漏洞，允許未經授權的攻擊者透過網路提升權限。
  - □CVE-2026-15409□SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability (CVSS v3.1: 10.0)
  - 【是否遭勒索軟體利用:未知□ SonicWall SMA1000 Appliances 存在伺服器端請求偽造漏洞，可能允許未經身分驗證的遠端攻擊者使裝置向非預期位置發送請求。
  - □CVE-2026-15410□SonicWall SMA1000 Appliances Code Injection Vulnerability (CVSS v3.1: 7.2)
  - 【是否遭勒索軟體利用:未知□ SonicWall SMA1000 Appliances 存在程式碼注入漏洞，在特定條件下，可能允許經身份驗證並具有管理員權限的遠端攻擊者執行任意作業系統指令。
  - □CVE-2026-46817□Oracle E-Business Suite Improper Privilege Management Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知□ Oracle E-Business Suite 存在權限管理不當漏洞，允許可透過 HTTP 存取系統的未經身分驗證攻擊者入侵 Oracle Payments□成功利用此漏洞可能導致 Oracle Payments 遭到接管。
  - □CVE-2023-4346□KNX Association KNX Protocol Connection Authorization Option 1 Overly Restrictive Account Lockout Mechanism Vulnerability (CVSS v3.1: 7.5)
  - 【是否遭勒索軟體利用:未知□ KNX Association KNX Protocol Connection Authorization Option 1 存在帳戶鎖定機制不當漏洞，可能允許攻擊者清除所有未啟用額外安全性選項的裝置，並設定BCU金鑰以鎖定裝置。
  - □CVE-2026-58644□Microsoft SharePoint Server Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知□ Microsoft SharePoint Server 存在不受信任資料反序列化漏洞，可能允許未經授權的攻擊者透過網路執行程式碼。
  - □CVE-2026-25089□Fortinet FortiSandbox OS Command Injection Vulnerability (CVSS v3.1: 9.8)
  - 【是否遭勒索軟體利用:未知□ Fortinet FortiSandbox□FortiSandbox Cloud 及 FortiSandbox PaaS 的 Web UI 存在作業系統指令注入漏洞，可能允許未經身分驗證的攻擊者透過特製的 HTTP 請求執行未經授權的指令。

    - 【CVE-2026-39808】Fortinet FortiSandbox OS Command Injection Vulnerability (CVSS v3.1: 9.8)
    - 【是否遭勒索軟體利用:未知】 Fortinet FortiSandbox 的 API 端點存在作業系統指令注入漏洞，可能允許未經身分驗證的攻擊者透過特製的 HTTP 請求執行未經授權的程式碼或指令。
- 影響平台:
    - 【CVE-2008-4128】Cisco 871 Integrated Services Router 所使用之 Cisco IOS 12.4【涉及 HTTP Administration 元件。
    - 【CVE-2026-56155】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56155
    - 【CVE-2026-56164】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56164
    - 【CVE-2026-15409】請參考官方所列的影響版本 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008
    - 【CVE-2026-15410】請參考官方所列的影響版本 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008
    - 【CVE-2026-46817】請參考官方所列的影響版本 https://www.oracle.com/security-alerts/cspumay2026.html
    - 【CVE-2023-4346】請參考所列影響版本 https://www.cisa.gov/news-events/ics-advisories/icsa-23-236-01
    - 【CVE-2026-58644】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58644
    - 【CVE-2026-25089】請參考官方所列的影響版本 https://fortiguard.fortinet.com/psirt/FG-IR-26-141
    - 【CVE-2026-39808】請參考官方所列的影響版本 https://fortiguard.fortinet.com/psirt/FG-IR-26-100
- 建議措施:
    - 【CVE-2008-4128】 受影響產品可能已達生命週期終止【EoL】和／或服務終止【EoS】階段，建議使用者停止使用該產品。 https://www.cisco.com/c/en/us/obsolete/ios-nx-os-software/cisco-ios-software-releases-12-4-mainline.html
    - 【CVE-2026-56155】 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/vulnerability/CVE-2026-56155
    - 【CVE-2026-56164】 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/vulnerability/CVE-2026-56164
    - 【CVE-2026-15409】 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-2026-0008
    - 【CVE-2026-15410】 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-2026-0008
    - 【CVE-2026-46817】 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/cspumay2026.html
    - 【CVE-2023-4346】 官方已針對漏洞釋出緩解措施 https://www.cisa.gov/news-events/ics-advisories/icsa-23-236-01
    - 【CVE-2026-58644】 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/vulnerability/CVE-2026-58644
    - 【CVE-2026-25089】 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-26-141
    - 【CVE-2026-39808】 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-26-100

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:20260724_21

Last update: **2026/07/24 10:14**