張貼日期：2026/08/07

【漏洞預警CISA新增3個已知遭駭客利用之漏洞至KEV目錄(2026/07/27-2026/08/02)

- 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(2026/07/27-2026/08/02)

- 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-200-202608-00000001
  - CVE-2025-68686Fortinet FortiOS Exposure of Sensitive Information to an Unauthorized Actor Vulnerability (CVSS v3.1: 5.9)
  - 【是否遭勒索軟體利用:未知 Fortinet FortiOS存在Exposure of Sensitive Information to an Unauthorized Actor漏洞，可能允許未經授權的遠端攻擊者透過特製的HTTP請求繞過針對某些漏洞利用後案例中觀察到的符號連結持久化機制所開發的修補程式。攻擊者必須先透過案系統層級的其他漏洞成功入侵該產品，才能利用此漏洞。
  - CVE-2026-16812Arista VeloCloud Orchestrator On-Prem OS Command Injection Vulnerability (CVSS v3.1: 10.0)
  - 【是否遭勒索軟體利用:未知 Arista VeloCloud Orchestrator On-Prem 存在作業系統指令注入漏洞，可能允許遠端攻擊者存取內部特權功能，並對VCO主機造成影響。若此漏洞遭成功利用，可能會危及Orchestrator及其所管理資料的機密性、完整性與可用性。
  - CVE-2026-20316Cisco Secure Firewall Management Center Use of Hard-coded Password Vulnerability (CVSS v3.1: 5.3)
  - 【是否遭勒索軟體利用:未知 Cisco Secure Firewall Management Center存在使用硬編碼密碼漏洞，可能允許未經驗證的遠端攻擊者使用低權限帳號登入受影響的裝置，並存取受影響系統內的敏感資料。
- 影響平台:
  - CVE-2025-68686請參考官方所列的影響版本 https://fortiguard.fortinet.com/psirt/FG-IR-25-934
  - CVE-2026-16812請參考官方所列的影響版本 https://www.arista.com/en/support/advisories-notices/security-advisory/24364-security-advisory-0144
  - CVE-2026-20316請參考官方所列的影響版本 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-static-cred-BET3Cjh
- 建議措施:
  - CVE-2025-68686 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-25-934
  - CVE-2026-16812 官方已針對漏洞釋出修復更新，請更新至相關版本 https://www.arista.com/en/support/advisories-notices/security-advisory/24364-security-advisory-0144
  - CVE-2026-20316 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-fmc-static-cred-BET3Cjh

---

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:20260807_21

Last update: **2026/08/07 09:17**