**張貼日期：2025/08/05**

# 【漏洞預警】CISA新增3個已知遭駭客利用之漏洞至KEV目錄(2025/07/28-2025/08/03)

- 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(2025/07/28-2025/08/03)

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202508-00000001
  1. 【CVE-2023-2533】PaperCut NG/MF Cross-Site Request Forgery (CSRF) Vulnerability (CVSS v3.1: 8.4)
     - 【是否遭勒索軟體利用:未知】PaperCut NG/MF存在跨站請求偽造漏洞，在特定條件下，攻擊者可能利用此漏洞修改安全設定或執行任意程式碼。
     - 【影響平台】請參考官方所列的影響版本
     - https://www.papercut.com/kb/Main/SecurityBulletinJune2023
  2. 【CVE-2025-20337】Cisco Identity Services Engine Injection Vulnerability (CVSS v3.1: 10.0)
     - 【是否遭勒索軟體利用:未知】Cisco Identity Services Engine(ISE)和Cisco ISE-PIC中的特定API因未充分驗證使用者提供的輸入而存在注入漏洞。攻擊者可藉由提交特製的 API 請求來利用此漏洞。若成功被利用，該漏洞可能允許攻擊者在受影響的裝置上執行遠端程式碼並取得root權限。
     - 【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-ise-unauth-rce-ZAd2GnJ6
  3. 【CVE-2025-20281】Cisco Identity Services Engine Injection Vulnerability (CVSS v3.1: 10.0)
     - 【是否遭勒索軟體利用:未知】Cisco Identity Services Engine(ISE)和Cisco ISE-PIC中的特定API因未充分驗證使用者提供的輸入而存在注入漏洞。攻擊者可藉由提交特製的 API 請求來利用此漏洞。若成功被利用，該漏洞可能允許攻擊者在受影響的裝置上執行遠端程式碼並取得root權限。
     - 【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-ise-unauth-rce-ZAd2GnJ6
- 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-2023-2533】 官方已針對漏洞釋出修復更新，請更新至相關版本
     - https://www.papercut.com/kb/Main/SecurityBulletinJune2023
  2. 【CVE-2025-20337】 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-ise-unauth-rce-ZAd2GnJ6
  3. 【CVE-2025-20281】 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-ise-unauth-rce-ZAd2GnJ6

---

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:20250805_02**

Last update: **2025/08/05 17:10**