張貼日期：2025/04/09

【漏洞預警】Ivanti 旗下設備存在重大資安漏洞(CVE-2025-22457)，並被積極利用於攻擊活動

- 主旨說明:【漏洞預警】Ivanti 旗下設備存在重大資安漏洞(CVE-2025-22457)，並被積極利用於攻擊活動
- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202504-00000003，
  - Ivanti 針對旗下產品 Connect Secure, Pulse Connect Secure(End-of-Support as of 2024/12/31), Policy Secure 及 ZTA Gateways 發布重大資安漏洞公告(CVE-2025-22457，CVSS評分9.0)。該漏洞由緩衝區溢位弱點所造成，允許未經身分驗證的遠端攻擊者可遠端執行任意程式碼 (RCE)，包括執行 Shell腳本程式與部署惡意程式等，建議用戶儘速採取防護措施，以降低潛在風險，並密切關注官方更新資訊。
- 影響平台:
  - Ivanti Connect Secure 22.7R2.5 及之前的版本
  - Pulse Connect Secure (End-of-Support) 9.1R18.9 及之前的版本
  - Ivanti Policy Secure 22.7R1.3 及之前的版本
  - ZTA Gateways 22.8R2 及之前的版本
- 建議措施:
  1. 官方已釋出修補，若有使用以上受影響之產品型號，請參考以下官方網址進行確認：https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457?language=en_US
  2. 目前已公告的修補資訊如下：
     - Ivanti Connect Secure: 更新 2025/2 發布的 22.7R2.6 安全性修補程式。
     - Pulse Connect Secure 9.1x: 該軟體已終止支援，請聯繫 Ivanti 進行軟體遷移。
     - Ivanti Policy Secure and ZTA Gateways: 安全性修補程式正在開發中，預計於4/21與4/19發布。
  3. 透過官網提供的工具針對系統進行完整性檢查：https://forums.ivanti.com/s/article/KB44755?language=en_US
- 參考資料: https://www.twcert.org.tw/tw/cp-169-10059-bec63-1.html

---

計算機與通訊中心
網路系統組 敬啟