張貼日期：2025/09/12

【漏洞預警Ivanti 旗下Connect SecurePolicy SecureZTA Gateways和 Neurons for Secure Access存在多個重大資安漏洞

- 主旨說明：【漏洞預警Ivanti 旗下Connect SecurePolicy SecureZTA Gateways和 Neurons for Secure Access存在多個重大資安漏洞

- 內容說明：
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202509-00000007
  - CVE-2025-55141CVSS8.8 此漏洞在受影響設備中缺乏授權機制，允許經過身分驗證且具有唯讀管理者權限的攻擊者修改與身分驗證相關的設定。
  - CVE-2025-55142CVSS8.8 此漏洞在受影響設備中缺乏授權機制，允許經過身分驗證且具有唯讀管理者權限的攻擊者修改與身分驗證相關的設定。
  - CVE-2025-55145CVSS8.9 此漏洞在受影響設備中缺乏授權機制，允許經過身分驗證的遠端攻擊者，劫持現有的HTML5連線。
  - CVE-2025-55147CVSS8.8 此漏洞在受影響設備中存在CSRF漏洞，允許經過身分驗證的遠端攻擊者，以受害者用戶的身分執行敏感性操作。
- 影響平台：
  - Ivanti Connect Secure 22.7R2.8 (含)之前版本
  - Ivanti Policy Secure 22.7R1.5 (含)之前版本
  - Ivanti ZTA Gateway 2.8R2.2 (含)之前版本
  - Ivanti Neurons for Secure Accessway 22.8R1.3 (含)之前版本
- 建議措施：
  - 請更新至以下版本：
  - Ivanti Connect Secure 22.7R2.9
  - Ivanti Connect Secure 22.8R2
  - Ivanti Policy Secure 22.7R1.6
  - Ivanti ZTA Gateway 2.8R2.3-723
  - Ivanti Neurons for Secure Accessway 22.8R1.4
- 參考資料：
  1. September Security Advisory Ivanti Connect Secure, Policy Secure, ZTA Gateways and Neurons for Secure Access (Multiple CVEs) https://forums.ivanti.com/s/article/September-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-and-Neurons-for-Secure-Access-Multiple-CVEs
  2. CVE-2025-55141 https://nvd.nist.gov/vuln/detail/CVE-2025-55141
  3. CVE-2025-55142 https://nvd.nist.gov/vuln/detail/CVE-2025-55142
  4. CVE-2025-55145 https://nvd.nist.gov/vuln/detail/CVE-2025-55145
  5. CVE-2025-55147 https://nvd.nist.gov/vuln/detail/CVE-2025-55147

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:20250912_05

Last update: **2025/09/12 15:24**