

張貼日期：2025/01/15

# 【漏洞預警】Ivanti部分產品存在安全漏洞(CVE-2025-0282)請儘速確認並進行修補

- 主旨說明: 【漏洞預警】Ivanti部分產品存在安全漏洞(CVE-2025-0282)請儘速確認並進行修補
- 內容說明:
  - 轉發 國家資安資訊分享與分析中心 NISAC-200-202501-00000001
  - 研究人員發現Ivanti部分產品存在緩衝區溢位(Buffer Overflow)(CVE-2025-0282)漏洞，允許未經身分鑑別之遠端攻擊者利用此漏洞執行任意程式碼。該漏洞已遭駭客利用，請儘速確認並進行修補。
- 影響平台:
  - Ivanti Connect Secure 22.7R2.5(不含)以前版本
  - Ivanti Policy Secure 22.7R1.2(不含)以前版本
  - Ivanti Neurons for ZTA gateways 22.7R2.3(不含)以前版本
- 建議措施: 官方已針對漏洞釋出修復更新，請參考官方說明，網址如下：  
[https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283?language=en\\_US](https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283?language=en_US)
- 參考資料:
  1. <https://nvd.nist.gov/vuln/detail/CVE-2025-0282>
  2. [https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283?language=en\\_US](https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283?language=en_US)
  3. <https://labs.watchtowr.com/exploitation-walkthrough-and-techniques-ivanti-connect-secure-rce-cve-2025-0282/>

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/mailling:announcement:20250115\\_01](https://net.nthu.edu.tw/netsys/mailling:announcement:20250115_01)



Last update: **2025/01/15 14:35**