張貼日期：2026/09/03

【漏洞預警】NetScaler ADC與NetScaler Gateway存在高風險安全漏洞(CVE-2026-19490)，請儘速確認並進行修補

- 主旨說明:【漏洞預警】NetScaler ADC與NetScaler Gateway存在高風險安全漏洞(CVE-2026-19490)，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 資安訊息警訊 NISAC-200-202608-00000011
  - 研究人員發現NetScaler ADC與NetScaler Gateway存在身分鑑別繞過(Authentication Bypass)漏洞(CVE-2026-19490)，當設備設定為Gateway(SSL VPN、ICA Proxy、CVPN或RDP Proxy)或AAA虛擬伺服器時，未經身分鑑別之遠端攻擊者可藉由替代路徑繞過身分鑑別機制，請儘速確認並進行修補。
- 影響平台:
  - NetScaler ADC與NetScaler Gateway 14.1-x至14.1-73.32(不含)版本
  - NetScaler ADC與NetScaler Gateway 13.1-x至13.1-63.21(不含)版本
  - NetScaler ADC FIPS 14.1-73.32(不含)以前版本
  - NetScaler ADC FIPS與NDcPP 13.1-37.277(不含)以前版本
  - 使用NetScaler執行個體之Secure Private Access for Hybrid Deployments
- 建議措施:
  - 官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下：https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696939
- 參考資料:
  1. https://nvd.nist.gov/vuln/detail/CVE-2026-19490
  2. https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696939

計算機與通訊中心
網路系統組 敬啟