

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026082703084646	發佈時間	2026-08-27 15:54:47
事故類型	ANA-漏洞預警	發現時間	2026-08-27 15:54:47
影響等級	中		
[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。 情資分享等級: WHITE(情資內容為可公開揭露之資訊) 此訊息僅發送到「區縣市網路中心」，煩請貴單位協助轉發與通知轄下各單位知悉			
[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>