

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026071609072424	發佈時間	2026-07-16 09:52:24
事故類型	ANA-漏洞預警	發現時間	2026-07-16 09:52:24
影響等級	中		
[主旨說明:] 【漏洞預警】 NetScaler ADC 與 NetScaler Gateway 存在多項高風險安全漏洞(CVE-2026-8451、CVE-2026-8452、CVE-2026-8655、CVE-2026-10816、CVE-2026-10817 及 CVE-2026-13474)，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-200-202607-00000004 研究人員發現 NetScaler ADC 與 NetScaler Gateway 存在多項高風險安全漏洞 (CVE-2026-8451、CVE-2026-8452、CVE-2026-8655、CVE-2026-10816、CVE-2026-10817 及 CVE-2026-13474)，其中最嚴重之 CVE-2026-8452 為記憶體溢位(Memory Overflow)漏洞，當受影響裝置被設定為 Gateway 或 AAA Virtual Server 功能時，未經身分鑑別之遠端攻擊者可利用此漏洞造成系統異常、阻斷服務或其他非預期行為，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 至 14.1-72.61(不含)版本			

NetScaler ADC 與 NetScaler Gateway 13.1 至 13.1-63.18(不含)版本

NetScaler ADC FIPS 14.1-72.61(不含)以前版本

NetScaler ADC FIPS 與 NDcPP 13.1-37.272(不含)以前版本

[建議措施:]

官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下：

<https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604>

[參考資料:]

1. <https://nvd.nist.gov/vuln/detail/CVE-2026-8451>
2. <https://nvd.nist.gov/vuln/detail/CVE-2026-8452>
3. <https://nvd.nist.gov/vuln/detail/CVE-2026-8655>
4. <https://nvd.nist.gov/vuln/detail/CVE-2026-10816>
5. <https://nvd.nist.gov/vuln/detail/CVE-2026-10817>
6. <https://nvd.nist.gov/vuln/detail/CVE-2026-13474>
7. <https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604>