

ANA事件單通知:TACERT-ANA-2025090409095555【漏洞預警】CISA新增5個已知遭駭客利用之漏洞至KEV目錄(2025/08/25-2025/08/31)

教育機構ANA通報平台

發佈編號	TACERT-ANA-2025090409095555	發佈時間	2025-09-04 09:37:55
事故類型	ANA-漏洞預警	發現時間	2025-09-04 09:37:55
影響等級	低		
[主旨說明:]【漏洞預警】CISA新增5個已知遭駭客利用之漏洞至KEV目錄(2025/08/25-2025/08/31)			
[內容說明:] 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202509-00000001 1. 【CVE-2025-48384】Git Link Following Vulnerability (CVSS v3.1: 8.0) 【是否遭勒索軟體利用:未知】 Git存在連結追蹤漏洞，該漏洞源於Git對設定檔中carriage return characters的處理不一致。 【影響平台】請參考官方所列的影響版本 https://github.com/git/git/security/advisories/GHSA-vwqx-4fm8-6qc9 2. 【CVE-2024-8068】Citrix Session Recording Improper Privilege Management Vulnerability (CVSS v3.1: 8.0) 【是否遭勒索軟體利用:未知】 Citrix Session Recording存在權限管理不當漏洞，可能導致權限提升至NetworkService帳戶存取層級。 【影響平台】請參考官方所列的影響版本 https://support.citrix.com/support-home/home 3. 【CVE-2024-8069】Citrix Session Recording Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 8.0) 【是否遭勒索軟體利用:未知】 Citrix Session Recording存在未經信任資料反序列化漏洞，可能允許在NetworkService帳戶權限下執行有限的遠端程式碼。 【影響平台】請參考官方所列的影響版本 https://support.citrix.com/support-home/home			

4. 【CVE-2025-7775】Citrix NetScaler Memory Overflow Vulnerability (CVSS v3.1: 9.8)

【是否遭勒索軟體利用:未知】 Citrix NetScaler ADC和NetScaler Gateway存在記憶體溢位漏洞，可能導致遠端程式碼執行及/或阻斷服務攻擊。

【影響平台】請參考官方所列的影響版本

<https://support.citrix.com/support-home/home>

5. 【CVE-2025-57819】Sangoma FreePBX Authentication Bypass Vulnerability (CVSS v4.0: 10.0)

【是否遭勒索軟體利用:未知】 Sangoma FreePBX存在身分驗證繞過漏洞，由於在處理使用者提供的輸入資料時未進行充分的驗證與清理，攻擊者可在未經驗證的情況下存取 FreePBX 管理介面，進而引發任意資料庫操作及遠端程式碼執行。

【影響平台】請參考官方所列的影響版本

<https://github.com/FreePBX/security-reporting/security/advisories/GHSA-m42g-xg4c-5f3h>

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:]

詳細內容於內容說明欄之影響平台

[建議措施:]

1. 【CVE-2025-48384】 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://github.com/git/git/security/advisories/GHSA-vwqx-4fm8-6qc9>

2. 【CVE-2024-8068】 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://support.citrix.com/support-home/home>

3. 【CVE-2024-8069】 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://support.citrix.com/support-home/home>

4. 【CVE-2025-7775】 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://support.citrix.com/support-home/home>

5. 【CVE-2025-57819】 官方已針對漏洞釋出修復更新，請更新至相關版本

<https://github.com/FreePBX/security-reporting/security/advisories/GHSA-m42g-xg4c-5f3h>

[參考資料:]

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組

網址：<https://info.cert.tanet.edu.tw/>

專線電話：07-5250211

網路電話：98400000

E-Mail：service@cert.tanet.edu.tw