

教育機構 ANA 通報平台

|                                                                                                                                                                                                                                                                                                                                          |                             |      |                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|------|------------------------|
| 發佈編號                                                                                                                                                                                                                                                                                                                                     | TACERT-ANA-2025102201101414 | 發佈時間 | 2025-10-22<br>13:15:14 |
| 事故類型                                                                                                                                                                                                                                                                                                                                     | ANA-漏洞預警                    | 發現時間 | 2025-10-22<br>13:15:14 |
| 影響等級                                                                                                                                                                                                                                                                                                                                     | 中                           |      |                        |
| <b>[主旨說明:]</b> 【漏洞預警】Apache ActiveMQ NMS AMQP 存在高風險安全漏洞(CVE-2025-54539)，請儘速確認並進行修補                                                                                                                                                                                                                                                       |                             |      |                        |
| <b>[內容說明:]</b><br><br>轉發 國家資安資訊分享與分析中心 NISAC-200-202510-00000201<br><br>研究人員發現 Apache ActiveMQ NMS AMQP 用戶端存在反序列化不受信任資料(Deserialization of Untrusted Data)漏洞(CVE-2025-54539)。未經身分鑑別之遠端攻擊者可在受影響用戶端與不受信任之 AMQP 伺服器建立連線時，回傳特製序列化資料即可於用戶端執行任意程式碼，請儘速確認並進行修補。<br><br>情資分享等級: WHITE(情資內容為可公開揭露之資訊)<br><br>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 |                             |      |                        |
| <b>[影響平台:]</b><br><br>Apache ActiveMQ NMS AMQP 2.3.0(含)以前版本                                                                                                                                                                                                                                                                              |                             |      |                        |
| <b>[建議措施:]</b><br><br>請更新 Apache ActiveMQ NMS AMQP 至 2.4.0(含)以後版本                                                                                                                                                                                                                                                                        |                             |      |                        |
| <b>[參考資料:]</b>                                                                                                                                                                                                                                                                                                                           |                             |      |                        |

1. <https://nvd.nist.gov/vuln/detail/CVE-2025-54539>
2. <https://lists.apache.org/thread/9k684j07ljrshy3hxwhj5m0xjmkz1g2n>