

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2025112602112323	發佈時間	2025-11-26 14:04:24
事故類型	ANA-漏洞預警	發現時間	2025-11-26 14:04:24
影響等級	中		
[主旨說明:]【漏洞預警】ASUS DSL 路由器存在高風險安全漏洞(CVE-2025-59367)，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-200-202511-00000204 研究人員發現 ASUS 部分 DSL 型號路由器存在身分鑑別繞過(Authentication Bypass)漏洞(CVE-2025-59367)。 未經身分鑑別之遠端攻擊者可透過此漏洞，對受影響設備執行未經授權之存取，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:] DSL-AC51 DSL-AC750 DSL-N16			

[建議措施:]

官方已針對漏洞釋出修復更新，請更新至以下版本：

ASUS DSL-AC51 Firmware 1.1.2.3_1010 版本

ASUS DSL-AC750 Firmware 1.1.2.3_1010 版本

ASUS DSL-N16 Firmware 1.1.2.3_1010 版本

官方針對已停止支援(EOL)之設備提出安全建議，請參考官方說明，網址如下：
<https://www.asus.com/security-advisory>

[參考資料:]

1. <https://nvd.nist.gov/vuln/detail/CVE-2025-59367>
2. <https://www.asus.com/security-advisory>