

張貼日期：2025/11/26

【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

- 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。
- 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>

計算機與通訊中心
網路系統組 敬啟

From:
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/mailling:announcement:20251126_06

Last update: 2025/11/26 15:02

