**張貼日期：2026/09/10**

# 【漏洞預警】Microsoft Exchange Server存在高風險安全漏洞(CVE-2026-62911)，請儘速確認並進行修補

- 主旨說明:【漏洞預警】Microsoft Exchange Server存在高風險安全漏洞(CVE-2026-62911)，請儘速確認並進行修補

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 資安訊息警訊 NISAC-200-202609-00000007
  - 研究人員發現Microsoft Exchange Server存在身分鑑別繞過(Authentication Bypass)漏洞(CVE-2026-62911)，已通過身分鑑別之遠端攻擊者可誘使使用者操作特製內容，用以攔截並重送身分鑑別憑證，藉此繞過伺服器之身分鑑別機制，進而提升權限並取得伺服器上使用者信箱之存取權，請儘速確認並進行修補。
- 影響平台:
  - Microsoft Exchange Server 2016 Cumulative Update 23 15.01.2507.072(不含)以前版本
- 建議措施:
  - 官方已針對漏洞釋出修補程式，請更新至下列版本 Microsoft Exchange Server 2016 Cumulative Update 23 15.01.2507.072(含)以後版本 Microsoft Exchange Server 2019 Cumulative Update 14 15.02.1544.044(含)以後版本 Microsoft Exchange Server 2019 Cumulative Update 15 15.02.1748.049(含)以後版本 Microsoft Exchange Server Subscription Edition RTM 15.02.2562.046(含)以後版本
  - 詳細說明請參考官方公告，網址如下：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62911
- 參考資料:
  1. https://nvd.nist.gov/vuln/detail/CVE-2026-62911
  2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62911

---

計算機與通訊中心
網路系統組 敬啟