張貼日期：2024/08/01

【漏洞預警】Cisco Secure Email Gateway存在高風險安全漏洞(CVE-2024-20401)，請儘速確認並進行修補

- 主旨說明：Cisco Secure Email Gateway存在高風險安全漏洞(CVE-2024-20401)，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 NISAC-200-202407-00000209，
  - 研究人員發現Cisco Secure Email Gateway之Content Scanner Tools存在任意檔案寫入(Arbitrary File Write)漏洞(CVE-2024-20401)，允許未經身分鑑別之遠端攻擊者，藉由寄送帶有特製附件之惡意郵件觸發漏洞，進而新增管理者帳號、執行任意程式碼及發動阻斷服務攻擊(DoS)，
- 影響平台：
  - Content Scanner Tools 23.3.0.4823(不含)以前版本
- 建議措施：
  - 官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-bGG2UsjH
- 參考資料：
  1. https://nvd.nist.gov/vuln/detail/CVE-2024-20401
  2. https://www.recordedfuture.com/vulnerability-database/CVE-2024-20401
  3. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-bGG2UsjH

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/mailing:announcement:20240801_01

Last update: **2024/08/01 11:16**