張貼日期：2026/04/28

【漏洞預警Cisco旗下Integrated Management Controller 存在2個重大資安漏洞

- 主旨說明:【漏洞預警Cisco旗下Integrated Management Controller 存在2個重大資安漏洞

- 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 TWCERTCC-200-202604-00000004
  - Cisco 旗下整合管理控制器(Integrated Management ControllerIMC)是一款專門為Cisco整合運算系統的伺服器設計管理工具，提供伺服器遠端監控、配置和管理功能，近日Cisco發布重大資安公告(CVE-2026-20093CVSS9.8 和 CVE-2026-20094CVSS8.8)
  - CVE-2026-20093為身分驗證繞過漏洞，可能允許未經身分驗證的遠端攻擊者繞過身分驗證，並以管理員身分存取系統CVE-2026-20094存在於IMC的Web管理介面，此為命令注入漏洞，經身分驗證的遠端攻擊者可能在受影響的底層作業系統上，執行任意程式碼或命令，並將權限提升至root
- 影響平台:
  - Cisco 5000 Series ENCS 4.15(含)之前版本
  - Cisco Catalyst 8300 Series Edge uCPE 4.16(含)之前版本
  - Cisco Catalyst 8300 Series Edge uCPE 4.18版本
  - UCS C-Series M5 Rack Server 4.2(含)之前版本
  - UCS C-Series M5 Rack Server 4.3版本
  - UCS C-Series M6 Rack Server 4.2(含)之前版本
  - UCS C-Series M6 Rack Server 4.3
  - UCS C-Series M6 Rack Server 6.0
  - UCS E-Series M3 3.2 (含)之前版本
  - UCS E-Series M6 4.15 (含)之前版本
- 建議措施:
  - 根據官方網站釋出的解決方式進行修補
  - CVE-2026-20093 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass-AgG2BxTn
  - CVE-2026-20094 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-3hKN3bVt
- 參考資料:
  1. https://www.twcert.org.tw/tw/cp-169-10823-4db55-1.html

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:20260428_24

Last update: **2026/04/28 10:56**