國立成功大學 National Cheng Kung University

ANA事件單通知:TACERT-ANA-202604100204393【漏洞預警】Cisco旗下Integrated Management Controller 存在2個重大資安漏洞

教育機構ANA通報平台

發佈編號	TACERT-ANA-2026041002043939	發佈時間	2026-04-10 14:19:40
事故類型	ANA-漏洞預警	發現時間	2026-04-10 14:19:40
影響等級	低		

[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 Controller，IMC)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-2026-20093，CVSS：9.8 和 CVE-2026-20094，CVSS：8.8)。

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。

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:]

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

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組
網址：https://info.cert.tanet.edu.tw/
專線電話：07-5250211
網路電話：98400000
E-Mail：service@cert.tanet.edu.tw