

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026030503034747	發佈時間	2026-03-05 15:05:57
事故類型	ANA-漏洞預警	發現時間	2026-03-05 15:05:57
影響等級	低		
【主旨說明:】 【漏洞預警】Cisco 旗下防火牆系統存在 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-200-202603-00000004			
<p>Cisco Secure Firewall Management Center (FMC) 是一套集中式管理平台，用於統一管理與監控 Cisco 防火牆產品，提供完整的威脅防禦視野，並支援政策制定、事件分析、流量監控與裝置設定等功能，近日 Cisco 發布重大資安公告。</p>			
<p>【CVE-2026-20131，CVSS：10.0】 此漏洞存在於 FMC 的網頁管理介面，未經身分驗證的遠端攻擊者，可能以 root 身分執行任意 Java 程式碼。</p>			
<p>【CVE-2026-20079，CVSS：10.0】 此漏洞存在於 FMC 的網頁管理介面，未經身分驗證的遠端攻擊者，可能繞過身分驗證並在受影響的裝置執行腳本，從而獲得對底層作業系統的 root 存取權限。</p>			
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 Secure Firewall Management Center (FMC) 6.4.0.13、6.4.014、
6.4.0.15、6.4.0.16、6.4.0.17、6.4.0.18、7.0.0、7.0.0.1、7.0.1、
7.0.1.1、70.2、7.0.2.1、7.0.3、7.0.4、7.0.5、7.0.6、7.0.6.1、
7.0.6.2、7.0.6.3、7.0.7、7.0.8、7.0.8.1、7.1.0、7.1.0.1、7.1.0.2、
7.1.0.3、7.2.0、7.2.1、7.2.2、7.2.0.1、7.2.3、7.2.3.1、7.2.4、
7.2.4.1、7.2.5、7.2.5.1、7.2.6、7.2.7、7.2.5.2、7.2.8、7.2.8.1、
7.2.9、7.2.10、7.2.10.2、7.2.10.1、7.3.0、7.3.1、7.3.1.1、7.3.1.2、
7.4.0、7.4.1、7.4.1.1、74.2、7.4.2.1、7.4.2.2、7.4.2.3、7.4.2.4、
7.4.3、7.4.4、7.4.5、7.6.0、7.6.1、7.6.2、7.6.2.1、7.6.3、7.6.4、
7.7.0、7.7.10、7.7.10.1、7.7.11、10.0.0 版本

[建議措施:]

依官方網站釋出的解決方式進行修補：

【CVE-2026-20131】

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh>

【CVE-2026-20079】

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2>

[參考資料:]

1. <https://www.twcert.org.tw/tw/cp-169-10747-660ee-1.html>