

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026100203101919	發佈時間	2026-10-02 15:18:20
事故類型	ANA-漏洞預警	發現時間	2026-10-02 15:18:20
影響等級	中		
[主旨說明:] 【漏洞預警】Cisco Secure FMC 存在高風險安全漏洞(CVE-2026-20242 與 CVE-2026-20324)，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 資安訊息警訊 NISAC-200-202610-00000002 研究人員發現 Cisco Secure FMC 存在多項高風險安全漏洞(CVE-2026-20242 與 CVE-2026-20324)，類型分別為不安全之反序列化(Insecure Deserialization) 與不當存取控制(ImproperAccess Control)，請儘速確認並進行修補。 【CVE-2026-20242】 當啟用外部資料庫存取(External Database Access)功能，且存取清單中已設定主機時，未經身分鑑別之遠端攻擊者可從清單內之主機向特定 TCP 連接埠傳送特製之 Java 序列化位元組串流，進而於受影響裝置以 root 權限執行任意指令。 【CVE-2026-20324】 當啟用 sftunnel 通訊協定時(系統預設為啟用)，已通過身分鑑別之遠端攻擊者可藉由劫持 sftunnel 連線，或冒用合法註冊之 sftunnel 對端身分傳送指令，將惡意檔案寫入裝置任意位置，並以 root 權限執行任意程式碼。 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 FMC 7.0.0 至 7.0.9、7.2.0 至 7.2.11、7.3.0 至 7.3.1.2、7.4.0 至 7.4.7、7.6.0 至 7.6.5、7.7.0 至 7.7.12 及 10.0.0 至 10.0.1 版本

[建議措施:]

官方已針對漏洞釋出修補或更新，請參考官方說明進行處置，網址如下：

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-javarce-y2NypXwk>

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sftunn-codex-c3O4Jft2>

[參考資料:]

1. <https://nvd.nist.gov/vuln/detail/CVE-2026-20242>
2. <https://nvd.nist.gov/vuln/detail/CVE-2026-20242>
3. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-javarce-y2NypXwk>
4. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sftunn-codex-c3O4Jft2>
5. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-notice-jfxK98ZP>