

張貼日期：2026/10/05

【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

- 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(Improper Access 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。
- 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-c304jft2>
- 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-c304jft2>
 5. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-notice-jfxK98ZP>

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:20261005_23



Last update: **2026/10/05 12:22**