張貼日期：2021/06/29

【資安漏洞預警□Palo Alto Networks之Cortex XSOAR產品存在安全漏洞(CVE-2021-3044)□請儘速確認並進行更新

主旨：【資安漏洞預警□Palo Alto Networks之Cortex XSOAR產品存在安全漏洞(CVE-2021-3044)□允許攻擊者遠端執行未經授權之操作，請儘速確認並進行更新

- 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-ANA-202106-1362□
  - Cortex XSOAR為Palo Alto Networks推出之資安協調、自動化與回應平台，研究人員發現Cortex XSOAR存在安全漏洞(CVE-2021-3044)□遠端攻擊者可透過網路存取Cortex XSOAR服務器之REST API執行未經授權之操作。
- 影響平台：
  受影響Cortex XSOAR版本如下(其他版本，包含Cortex XSOAR 5.5, 6.0.0, 6.0.1及6.02不受影響)：
  - Cortex XSOAR 6.1.0□1016923(含)與1271064(不含)之間版本
  - Cortex XSOAR 6.2.0□1271065(不含)以前版本
- 建議措施：
  - 目前Palo Alto Networks官方已針對此漏洞釋出更新程式，請各機關聯絡設備維護廠商或參考下方網址進行更新：https://security.paloaltonetworks.com/CVE-2021-3044
- 參考資料：
  1. https://security.paloaltonetworks.com/CVE-2021-3044
  2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3044

計算機與通訊中心
網路系統組 敬啟