張貼日期：2023/06/20

【資安漏洞預警Fortinet FortiOS與FortiProxy存在高風險安全漏洞(CVE-2023-27997)請儘速確認並進行更新或評估採取緩解措施！

- 主旨說明Fortinet FortiOS與FortiProxy存在高風險安全漏洞(CVE-2023-27997)允許攻擊者在未經身分鑑別之情況下，遠端執行任意程式碼，請儘速確認並進行更新或評估採取緩解措施！
- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-ANA-202306-0180
  - 研究人員發現Fortinet FortiOS與FortiProxy之SSL-VPN功能存在堆積型緩衝區溢位(Heap-based Buffer Overflow)漏洞(CVE-2023-27997)允許攻擊者在未經身分鑑別之情況下，藉由發送特製之HTTP(S)請求來觸發此漏洞，進而遠端執行任意程式碼。
- 影響平台：
  - FortiOS-6K7K 7.0.10、7.0.5、6.4.12、6.4.10、6.4.8、6.4.6、6.4.2、6.2.9至6.2.13、6.2.6至6.2.7、62.4、6.0.12至6.0.16及6.0.10版本
  - FortiProxy 7.2.0至7.2.3、7.0.0至7.0.9、2.0.0至2.0.12、1.2所有版本及1.1所有版本
  - FortiOS 7.2.0至7.2.4、7.0.0至7.0.11、6.4.0至6.4.12、6.2.0至6.2.13及6.0.0至6.016版本
- 建議措施：
  1. 目前Fortinet官方已針對此漏洞釋出更新程式，請各機關儘速進行版本確認與更新(1)FortiOS-6K7K請升級至7.0.12、6.4.13、6.2.15及6.017(含)以上版本(2)FortiProxy請升級至7.2.4與7.0.10(含)以上版本(3)FortiOS請升級至7.4.0、7.2.5、7.0.12、6.4.13、6.2.14及6.0.17(含)以上版本
  2. 如未能及時更新，請參考Fortinet官方網頁之Workaround一節，採取關閉SSL-VPN功能之緩解措施。
- 參考資料：
  1. https://thehackernews.com/2023/06/critical-rce-flaw-discovered-in.html?&web_view=true
  2. https://www.fortiguard.com/psirt/FG-IR-23-097

計算機與通訊中心
網路系統組 敬啟