張貼日期：2023/03/15

【資安漏洞預警Fortinet FortiOS與FortiProxy存在高風險安全漏洞(CVE-2023-25610)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-2023-25610)允許攻擊者在未經身分鑑別之情況下，執行遠端任意程式碼或發動服務阻斷攻擊，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-202303-0736
  - 研究人員發現Fortinet FortiOS與FortiProxy之HTTP(S)管理介面存在緩衝區負位(buffer underflow)漏洞(CVE-2023-25610)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，或者透過圖形化介面(GUI)進行阻斷服務(DoS)攻擊。
- 影響平台:
  - 受影響版本如下：
    - FortiOS 7.2.0至7.2.3版本
    - FortiOS 7.0.0至7.0.9版本
    - FortiOS 6.4.0至6.4.11版本
    - FortiOS 6.2.0至6.2.12版本
    - FortiOS 6.0所有版本
    - FortiProxy 7.2.0至7.2.2版本
    - FortiProxy 7.0.0至7.0.8版本
    - FortiProxy 2.0.0至2.0.12版本
    - FortiProxy 1.2所有版本
    - FortiProxy 1.1所有版本
  - 下列使用受本漏洞影響FortiOS版本之設備僅受阻斷服務漏洞影響：
    - FortiGateRugged-100C
    - FortiGate-100D
    - FortiGate-200C
    - FortiGate-200D
    - FortiGate-300C
    - FortiGate-3600A
    - FortiGate-5001FA2
    - FortiGate-5002FB2
    - FortiGate-60D
    - FortiGate-620B
    - FortiGate-621B
    - FortiGate-60D-POE
    - FortiWiFi-60D
    - FortiWiFi-60D-POE
    - FortiGate-300C-Gen2
    - FortiGate-300C-DC-Gen2
    - FortiGate-300C-LENC-Gen2

    - FortiWiFi-60D-3G4G-VZW
    - FortiGate-60DH
    - FortiWiFi-60DH
    - FortiGateRugged-60D
    - FortiGate-VM01-Hyper-V
    - FortiGate-VM01-KVM
    - FortiWiFi-60D-I
    - FortiGate-60D-Gen2
    - FortiWiFi-60D-J
    - FortiGate-60D-3G4G-VZW
    - FortiWifi-60D-Gen2
    - FortiWifi-60D-Gen2-J
    - FortiWiFi-60D-T
    - FortiGateRugged-90D
    - FortiWifi-60D-Gen2-U
    - FortiGate-50E
    - FortiWiFi-50E
    - FortiGate-51E
    - FortiWiFi-51E
    - FortiWiFi-50E-2R
    - FortiGate-52E
    - FortiGate-40F
    - FortiWiFi-40F
    - FortiGate-40F-3G4G
    - FortiWiFi-40F-3G4G
    - FortiGate-40F-3G4G-NA
    - FortiGate-40F-3G4G-EA
    - FortiGate-40F-3G4G-JP
    - FortiWiFi-40F-3G4G-NA
    - FortiWiFi-40F-3G4G-EA
    - FortiWiFi-40F-3G4G-JP
    - FortiGate-40F-Gen2
    - FortiWiFi-40F-Gen2
- 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請升級至7.4.0、7.2.4、70.10、6.4.12及6.2.13(含)以上版本
        2. FortiProxy請升級至7.2.3與7.0.9(含)以上版本
        3. FortiOS-6K7K請升級至7.0.10、6.4.12、6.2.13(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，採取下列緩解措施：
        1. 關閉HTTP(S)管理介面。
        2. 限制可存取管理介面之IP。
- 參考資料:
    1. https://www.fortiguard.com/psirt/FG-IR-23-001
    2. https://www.helpnetsecurity.com/2023/03/09/cve-2023-25610/

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:20230315_01

Last update: **2023/03/15 14:02**