張貼日期：2024/03/07

【漏洞預警Fortinet FortiOS與FortiProxy存在高風險安全漏洞(CVE-2024-21762)請儘速確認並進行修補！

- 主旨說明Fortinet FortiOS與FortiProxy存在高風險安全漏洞(CVE-2024-21762)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 NISAC-200-202403-00000009
  - 研究人員發現Fortinet FortiOS與FortiProxy存在越界寫入(Out-of-Bounds Write)漏洞(CVE-2024-21762)允許未經身分鑑別的遠端攻擊者經由特製之HTTP請求，執行任意程式碼或命令。該漏洞目前已遭駭客利用，請儘速確認並進行修補。
- 影響平台:
  - FortiOS 7.4.0至7.4.2
  - FortiOS 7.2.0至7.2.6
  - FortiOS 7.0.0至7.0.13
  - FortiOS 6.4.0至6.4.14
  - FortiOS 6.2.0至6.2.15
  - FortiOS 6.0.0至6.0.17
  - FortiProxy 7.4.0至7.4.2
  - FortiProxy 7.2.0至7.2.8
  - FortiProxy 7.0.0至7.0.14
  - FortiProxy 2.0.0至2.0.13
  - FortiProxy 1.2所有版本
  - FortiProxy 1.1所有版本
  - FortiProxy 1.0所有版本
- 建議措施:
  - 官方已針對漏洞釋出修復更新，請更新至以下版本：
    - FortiOS 7.4.3(含)以上、7.2.7(含)以上、7.0.14(含)以上、6.4.15(含)、6.2.16(含)以上及6.0.18(含)以上版本
    - FortiProxy 7.4.3(含)以上、7.2.9(含)以上、7.0.15(含)以上及2.0.14(含)以上版本。至於1.2所有版本、1.1所有版本及1.0所有版本，請升級至前述有修補更新之版本。
- 參考資料:
  1. https://cwe.mitre.org/data/definitions/787.html
  2. https://www.fortiguard.com/psirt/FG-IR-24-015
  3. https://nvd.nist.gov/vuln/detail/CVE-2024-21762

—- 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:20240307_01

Last update: **2024/03/07 08:28**