

FW: 【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！

1 封郵件

gz710@mail.ncku.edu.tw <gz710@mail.ncku.edu.tw>
收件者: nckucc_黃國展 <gz710@mail.ncku.edu.tw>
副本: nckucc_朱敏清 <kkinglord@mail.ncku.edu.tw>

2024年3月7日 清晨7:56

各位老師好：

轉寄教育機構ANA通報平台通知 · 謝謝。

成大計網中心 敬上

連絡電話：06-2757575轉61037

From: service <service@cert.tanet.edu.tw>

Sent: Wednesday, March 6, 2024 4:37 PM

To: service@cert.tanet.edu.tw

Subject: (ANA事件單通知:TACERT-ANA-2024030604034545)(【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！)

教育機構ANA通報平台

發佈編號	TACERT-ANA-2024030604034545	發佈時間	2024-03-06 16:17:47
事故類型	ANA-漏洞預警	發現時間	2024-03-06 16:17:47
影響等級	中		
[主旨說明:] 【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！			
[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。 情資分享等級: WHITE(情資內容為可公開揭露之資訊) 此訊息僅發送到「區縣市網路中心」 · 煩請貴單位協助公告或轉發			
[影響平台:] <ul style="list-style-type: none">FortiOS 7.4.0至7.4.2FortiOS 7.2.0至7.2.6FortiOS 7.0.0至7.0.13FortiOS 6.4.0至6.4.14FortiOS 6.2.0至6.2.15FortiOS 6.0.0至6.0.17FortiProxy 7.4.0至7.4.2FortiProxy 7.2.0至7.2.8FortiProxy 7.0.0至7.0.14FortiProxy 2.0.0至2.0.13FortiProxy 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： <ul style="list-style-type: none">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:] <ol style="list-style-type: none">https://cwe.mitre.org/data/definitions/787.htmlhttps://www.fortiguard.com/psirt/FG-IR-24-015https://nvd.nist.gov/vuln/detail/CVE-2024-21762			

(此通報僅在於告知相關資訊 · 並非為資安事件) · 如果您對此通報的內容有疑問或有關於此事件的建議 · 歡迎與我們連絡。

教育機構資安通報應變小組
網址：<https://info.cert.tanet.edu.tw/>
專線電話：07-5250211
網路電話：98400000
E-Mail：service@cert.tanet.edu.tw