

張貼日期：2022/12/22

【資安漏洞預警】Fortinet FortiOS SSL-VPN存在高風險安全漏洞(CVE-2022-42475)請儘速確認並進行更新

- 主旨說明Fortinet FortiOS SSL-VPN存在高風險安全漏洞(CVE-2022-42475)允許未經授權之攻擊者遠端執行任意程式碼或指令，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 NISAC-ANA-202212-1296
 - 研究人員發現Fortinet FortiOS SSL-VPN存在緩衝區溢位漏洞(CVE-2022-42475)此漏洞已遭開採利用，未經授權之遠端攻擊者可藉由發送特製請求觸發此漏洞，進而執行任意程式碼或指令。
- 影響平台：
 - FortiOS 版本 7.2.0 到 7.2.2
 - FortiOS 版本 7.0.0 到 7.0.8
 - FortiOS 版本 6.4.0 到 6.4.10
 - FortiOS 版本 6.2.0 到 6.2.11
 - FortiOS 版本 6.0.0 到 6.0.15
 - FortiOS 版本 5.6.0至 5.6.14
 - FortiOS 版本 5.4.0 至5.4.13
 - FortiOS 版本 5.2.0 至 5.2.15
 - FortiOS 版本 5.0.0 至 5.0.14
 - FortiOS-6K7K 版本 7.0.0 至 7.0.7
 - FortiOS-6K7K 版本 6.4.0 至6.4.9
 - FortiOS-6K7K 版本 6.2.0 到 6.2.11
 - FortiOS-6K7K 版本 6.0.0 到 6.0.14
- 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6.0.16、6.2.12、6.4.11、7.0.9、7.2.3(含)以上版本
 2. FortiOS-6K7K請升級至6.0.15、6.2.12、6.4.10、7.0.8(含)以上版本
 2. 如未能及時更新，請關閉SSL-VPN以緩解此漏洞。
- 參考資料：
 1. <https://www.fortiguard.com/psirt/FG-IR-22-398>
 2. https://www.fisac.tw/STIX_CASE/QueryStixCase/Detail?Uno=4KbRA2xNjogYexcZfZB__s_D35r5e60Yc2iijyDPD2yrDo__e_
 3. <https://www.ithome.com.tw/news/154774>

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:20221222_01



Last update: **2022/12/22 16:06**