

張貼日期：2019/09/03

# 【資安漏洞預警】Pulse Connect Secure產品存在安全漏洞(CVE-2019-11510、CVE-2019-11539)

主旨：Pulse Connect Secure產品存在安全漏洞(CVE-2019-11510、CVE-2019-11539)允許未經授權使用者取得帳號與密碼，請儘速確認並進行更新

說明：

- 內容說明：  
資安公司BadPackets近期觀測發現駭客針對Pulse Secure公司之Pulse Connect Secure產品漏洞(CVE-2019-11510、CVE-2019-11539)進行大規模攻擊探測。  
攻擊者無需身分驗證即可遠端執行命令注入(Remote Command Injection)存取設備上之任意檔案如VPN帳號密碼檔案，進而利用所取得的認證資訊登入組織內部網路，進行橫向擴散。  
目前全球總計超過1萬4千個設備可能存在相關漏洞，其中台灣有217個受影響的設備。建議有使用受影響產品的用戶，升級至Pulse Secure官方所發布的修補版本。
- 影響平台：  
Pulse Connect Secure 9.0R1 - 9.0R3.3  
Pulse Connect Secure 8.3R1 - 8.3R7  
Pulse Connect Secure 8.2R1 - 8.2R12  
Pulse Connect Secure 8.1R1 - 8.1R15  
Pulse Policy Secure 9.0R1 - 9.0R3.3  
Pulse Policy Secure 5.4R1 - 5.4R7  
Pulse Policy Secure 5.3R1 - 5.3R12  
Pulse Policy Secure 5.2R1 - 5.2R12  
Pulse Policy Secure 5.1R1 - 5.1R15
- 建議措施：  
Pulse Secure已針對前述漏洞釋出修復版本，請聯絡設備維護廠商進行版本確認與更新，官方公告連結如下：
  1. [https://kb.pulsesecure.net/articles/Pulse\\_Security\\_Advisories/SA44101](https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101)
  2. [https://kb.pulsesecure.net/articles/Pulse\\_Technical\\_Bulletin/TSB44239](https://kb.pulsesecure.net/articles/Pulse_Technical_Bulletin/TSB44239)
- 參考資料：
  1. <https://badpackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/>
  2. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11510>
  3. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11539>

計算機與通訊中心  
網路系統組 敬啟

From:

<http://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

[http://net.nthu.edu.tw/netsys/mailling:announcement:20190903\\_01](http://net.nthu.edu.tw/netsys/mailling:announcement:20190903_01)

Last update: **2019/09/03 11:39**

