

張貼日期：2020/01/09

## 【資安漏洞預警】Citrix應用伺服器與閘道器產品存在安全漏洞(CVE-2019-19781)

主旨：Citrix應用伺服器與閘道器產品存在安全漏洞(CVE-2019-19781)可能被用於任意程式碼執行，請儘速確認並進行更新。

說明：

- 轉發國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202001-0226
- 資安公司Positive Technologies近期公布Citrix應用伺服器與閘道器產品存在安全漏洞(CVE-2019-19781)可能被用於任意程式碼執行(arbitrary code execution)進而允許未經授權使用者連入組織內部網路，建議有使用受影響產品的用戶，依Citrix原廠文件進行防護設定。
- 影響平台：
  - Citrix ADC and Citrix Gateway version 13.0 all supported builds
  - Citrix ADC and NetScaler Gateway version 12.1 all supported builds
  - Citrix ADC and NetScaler Gateway version 12.0 all supported builds
  - Citrix ADC and NetScaler Gateway version 11.1 all supported builds
  - Citrix NetScaler ADC and NetScaler Gateway version 10.5 all supported builds
- 建議措施：
  1. 依下列指令檢查Citrix伺服器設定，如果不是回應403 Forbidden表示可能存在漏洞。  
curl -k -l <https://Citrix伺服器網路位址/logon/LogonPoint/vpns/>  
curl -k -l <https://Citrix伺服器網路位址/logon/vpns/>  
curl -k -l <https://Citrix伺服器網路位址/vpn/vpns/>  
curl -k -l <https://Citrix伺服器網路位址/epa/vpns/>
  2. 依Citrix原廠發布建議措施，進行防護設定。  
<https://support.citrix.com/article/CTX267679>
  3. 檢查Citrix伺服器紀錄是否有異常登入或異常連線。
  4. 檢查資安防護設備紀錄是否有異常連線。
- 參考資料：
  1. <https://support.citrix.com/article/CTX267027>
  2. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19781>
  3. <https://www.ptsecurity.com/ww-en/about/news/citrix-vulnerability-allows-criminals-to-hack-networks-of-80000-companies>

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/ mailing:announcement:20200109\\_01](http://net.nthu.edu.tw/netsys/ mailing:announcement:20200109_01)

Last update: 2020/01/09 14:55



