張貼日期：2020/10/19

【資安漏洞預警】微軟Windows存在安全漏洞(CVE-2020-16898)□請儘速確認並進行更新！

主旨：【資安漏洞預警】微軟Windows TCP/IP堆疊存在安全漏洞(CVE-2020-16898)□允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新！

- 內容說明：
  - 轉發 行政院國家資通安全會報技術服務中心 資安訊息警訊 NISAC-ANA-202010-0502
  - 研究人員發現微軟Windows TCP/IP堆疊(TCP/IP stack)未能正確處理ICMPv6之路由器公告(Router Advertisement)封包，導致存在安全漏洞(CVE-2020-16898)□遠端攻擊者可藉由發送特製的ICMPv6路由器公告封包，利用此漏洞進而執行任意程式碼。
- 影響平台:
  受影響Windows版本如下:
  - Windows 10 Version 1709 for 32-bit Systems
  - Windows 10 Version 1709 for ARM64-based Systems
  - Windows 10 Version 1709 for x64-based Systems
  - Windows 10 Version 1803 for 32-bit Systems
  - Windows 10 Version 1803 for ARM64-based Systems
  - Windows 10 Version 1803 for x64-based Systems
  - Windows 10 Version 1809 for 32-bit Systems
  - Windows 10 Version 1809 for ARM64-based Systems
  - Windows 10 Version 1809 for x64-based Systems
  - Windows 10 Version 1903 for 32-bit Systems
  - Windows 10 Version 1903 for ARM64-based Systems
  - Windows 10 Version 1903 for x64-based Systems
  - Windows 10 Version 1909 for 32-bit Systems
  - Windows 10 Version 1909 for ARM64-based Systems
  - Windows 10 Version 1909 for x64-based Systems
  - Windows 10 Version 2004 for 32-bit Systems
  - Windows 10 Version 2004 for ARM64-based Systems
  - Windows 10 Version 2004 for x64-based Systems
  - Windows Server 2019
  - Windows Server 2019 (Server Core installation)
  - Windows Server, version 1903 (Server Core installation)
  - Windows Server, version 1909 (Server Core installation)
  - Windows Server, version 2004 (Server Core installation)
- 建議措施:
  1. 目前微軟官方已針對此漏洞釋出更新程式，請各機關聯絡設備維護廠商或參考以下建議進行更
     新：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898
  2. 如無法更新，亦可於Windows 1709以上版本環境中，執行□netsh int ipv6 set int *INTERFACENUMBER* rabaseddnsconfig=disable□之PowerShell指令，藉由停用ICMPv6 RDNSS功能，防止攻擊者進行弱點利用。
- 參考資料:

1. https://portalmsrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898
2. https://vuldb.com/?id.162598

- Q&A:
  1. Q如何確認所使用的Windows版本號？
     A以Windows 10為例，由 [開始] > [設定] > [系統] > [關於]，就可以看到Windows 10的版本資訊，圖文說明請參考https://www.jihsunbank.com.tw/newsite/web-atm/qa_5(37-1).htm
  2. Q如何進行重大更新？
     A以Windows 10為例，由 [開始] > [設定] > [更新與安全性] > [Windows Update] 請參考https://support.microsoft.com/zh-tw/help/4027667/windows-10-update

---

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:20201019_02

Last update: **2020/10/19 09:45**