張貼日期：2020/09/22

【資安漏洞預警Windows Netlogon遠端協定(MS-NRPC)存在安全漏洞，請儘速確認並進行更新

主旨：【漏洞預警Windows Netlogon遠端協定(MS-NRPC)存在安全漏洞(CVE-2020-1472)允許攻擊者在未授權之狀況下提權至網域管理者權限，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-202009-0830
  - 研究人員發現操作人員在使用Netlogon遠端協定(MS-NRPC)建立與網域控制站(Domain Controller)之安全通道時，存在可提升權限之安全漏洞(CVE-2020-1472)攻擊者在無任何網域登入帳密之狀況下，僅需針對存在漏洞之網域控制站(DC)建立安全通道連線，即可利用此漏洞變更網域管理員密碼並取得網域管理者權限，進而在該網域中之電腦執行任意程式碼。
- 影響平台:
  - Windows Server 2008 R2 for x64-based Systems Service Pack 1
  - Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
  - Windows Server 2012
  - Windows Server 2012 (Server Core installation)
  - Windows Server 2012 R2
  - Windows Server 2012 R2 (Server Core installation)
  - Windows Server 2016
  - Windows Server 2016 (Server Core installation)
  - 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:
  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：
  1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472
  2. https://support.microsoft.com/zh-tw/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc
- 參考資料:
  1. https://us-cert.cisa.gov/ncas/current-activity/2020/09/18/cisa-releases-emergency-directive-microsoft-windows-netlogon
  2. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472
  3. https://support.microsoft.com/zh-tw/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc
  4. https://www.ithome.com.tw/news/140014

計算機與通訊中心

網路系統組 敬啟