張貼日期：2020/07/16

【資安漏洞預警】微軟Windows DNS伺服器存在安全漏洞，請儘速確認並進行更新

主旨：【資安漏洞預警】微軟Windows DNS伺服器存在安全漏洞(CVE-2020-1350)攻擊者可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 (NCCST-ANA-G2020-0283)
  - 微軟Windows DNS伺服器存在安全漏洞(CVE-2020-1350)未經身分驗證的攻擊者可對DNS伺服器發送惡意請求，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 Server 2008 for 32-bit Systems Service Pack 2
  - Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
  - Windows Server 2008 for x64-based Systems Service Pack 2
  - Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
  - 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-2020-1350
  2. https://support.microsoft.com/zh-tw/help/4569509/windows-dns-server-remote-code-execution-vulnerability
  3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1350
- 參考資料:
  1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350
  2. https://support.microsoft.com/zh-tw/help/4569509/windows-dns-server-remote-code-execution-vulnerability
  3. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1350

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:20200716_02

Last update: **2020/07/16 16:09**