

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2021022010024848	發佈時間	2021-02-20 10:37:49
事故類型	ANA-漏洞預警	發現時間	2021-02-20 10:37:49
影響等級	中		

[主旨說明:] 【漏洞預警】微軟 Windows DNS 伺服器存在安全漏洞(CVE-2021-24078) , 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-202102-0954

研究人員發現微軟 Windows DNS 伺服器因輸入驗證不足 , 導致存在安全漏洞(CVE-2021-24078) , 遠端攻擊者可藉由發送特製封包 , 利用此漏洞進而執行任意程式碼。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

[影響平台:]

使用下列 Windows 作業系統之伺服器如啟用 DNS 服務 , 將受此漏洞影響 :

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 1909 (Server Core installation)
 Windows Server, version 2004 (Server Core installation)
 Windows Server, version 20H2 (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網址進行更新 :
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24078>

[參考資料:]

1. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24078>
2. <https://www.ithome.com.tw/news/142716>
3. <https://www.cybersecurity-help.cz/vdb/SB2021020934>
4. <https://thehackernews.com/2021/02/microsoft-issues-patches-for-in-wild-0html>
5. <https://www.nccst.nat.gov.tw/VulnerabilityDetail?lang=zh&seq=1144>