

ANA 事件單通知: TACERT-ANA- 2021111111114949)

【漏洞預警】微軟 Windows 作業系統與應用程式存在多個安全漏洞，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新!

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2021111111114949	發佈時間	2021-11-11 11:34:50
事故類型	ANA-漏洞預警	發現時間	2021-11-11 09:37:50
影響等級	中		
[主旨說明:] 【漏洞預警】微軟 Windows 作業系統與應用程式存在多個安全漏洞，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 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202111-0417 研究人員發現 Windows 作業系統與應用程式存在多個安全漏洞(CVE-2021-26443、38666、42292 及 42321)，遠端攻擊者可藉由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:] 一、CVE-2021-26443： ● Windows 10 Version 1809 for x64-based Systems ● Windows 10 Version 1909 for x64-based Systems ● Windows 10 Version 2004 for x64-based Systems ● Windows 10 Version 20H2 for x64-based Systems ● Windows 10 Version 21H1 for x64-based Systems ● Windows 11 for x64-based Systems ● Windows Server 2019 ● Windows Server 2019 (Server Core installation) 二、CVE-2021-38666： ● Remote Desktop client for Windows Desktop ● Windows 7 for 32-bit Systems Service Pack 1 ● Windows 7 for x64-based Systems Service Pack 1 ● Windows 8.1 for 32-bit systems			

- Windows 8.1 for x64-based systems
- Windows RT 8.1 Windows 10 for 32-bit Systems
- Windows 10 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 Version 1607 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 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 10 Version 20H2 for 32-bit Systems
- Windows 10 Version 20H2 for ARM64-based Systems
- Windows 10 Version 20H2 for x64-based Systems
- Windows 10 Version 21H1 for 32-bit Systems
- Windows 10 Version 21H1 for ARM64-based Systems

[建議措施:]

目前微軟官方已針對這些漏洞釋出更新程式，請各機關聯絡維護廠商或參考以下網址進行更新：

1. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26443>
2. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-38666>
3. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42292>
4. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42321>

[參考資料:]

1. <https://www.ithome.com.tw/news/147751>
2. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26443>
3. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-38666>

4. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42292>
5. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42321>

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組

網址：<https://info.cert.tanet.edu.tw/>

專線電話：07-5250211

網路電話：98400000

E-Mail：service@cert.tanet.edu.tw