

# 行政院國家資通安全會報技術服務中心

## 漏洞/資安訊息警訊

發布編號	NCCST-ANA-2021-0000551	發布時間	Wed Nov 10 16:33:29 CST 2021
事件類型	漏洞預警	發現時間	Wed Nov 10 00:00:00 CST 2021
警訊名稱	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	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。		
影響平台	受影響版本如下：  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)

Windows Server 2022

Windows Server 2022 (Server Core installation)

Windows Server, version 2004 (Server Core installation)

Windows Server, version 20H2 (Server Core Installation)

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

Windows 10 Version 21H1 for x64-based Systems

Windows 11 for ARM64-based Systems

Windows 11 for x64-based Systems

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 2022

Windows Server 2022 (Server Core installation)

Windows Server, version 2004 (Server Core installation)

Windows Server, version 20H2 (Server Core Installation)

CVE-2021-42292 :

Microsoft 365 Apps for Enterprise for 32-bit Systems

Microsoft 365 Apps for Enterprise for 64-bit Systems

Microsoft Excel 2013 RT Service Pack 1

Microsoft Excel 2013 Service Pack 1 (32-bit editions)

Microsoft Excel 2013 Service Pack 1 (64-bit editions)

Microsoft Excel 2016 (32-bit edition)

Microsoft Excel 2016 (64-bit edition)

Microsoft Office 2013 RT Service Pack 1

Microsoft Office 2013 Service Pack 1 (32-bit editions)

Microsoft Office 2013 Service Pack 1 (64-bit editions)

Microsoft Office 2016 (32-bit edition)

	<p>Microsoft Office 2016 (64-bit edition)</p> <p>Microsoft Office 2019 for 32-bit editions</p> <p>Microsoft Office 2019 for 64-bit editions</p> <p>Microsoft Office 2019 for Mac</p> <p>Microsoft Office LTSC 2021 for 32-bit editions</p> <p>Microsoft Office LTSC 2021 for 64-bit editions</p> <p>Microsoft Office LTSC for Mac 2021</p> <p>CVE-2021-42321 :</p> <p>Microsoft Exchange Server 2016 Cumulative Update 21</p> <p>Microsoft Exchange Server 2016 Cumulative Update 22</p> <p>Microsoft Exchange Server 2019 Cumulative Update 10</p> <p>Microsoft Exchange Server 2019 Cumulative Update 11</p>
影響等級	高
建議措施	<p>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：</p> <p>1. <a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42321">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42321</a></p>

	<p>1-26443</p> <p>2. <a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26443">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26443</a></p> <p>1-38666</p> <p>3. <a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-38666">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-38666</a></p> <p>1-42292</p> <p>4. <a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42292">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42292</a></p> <p>1-42321</p>
參考資料	<p>1. <a href="https://www.ithome.com.tw/news/147751">https://www.ithome.com.tw/news/147751</a></p> <p>2. <a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26443">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26443</a></p> <p>1-26443</p> <p>3. <a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-38666">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-38666</a></p> <p>1-38666</p> <p>4. <a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42292">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42292</a></p> <p>1-42292</p> <p>5. <a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42321">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42321</a></p> <p>1-42321</p>