

張貼日期：2021/09/17

【資安漏洞預警】微軟Windows作業系統存在多個安全漏洞，允許攻擊者取得權限或遠端執行任意程式碼，請儘速確認並進行更新！

- 主旨說明：【資安漏洞預警】微軟Windows作業系統存在多個安全漏洞，允許攻擊者取得權限或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-202109-0847
 - 研究人員發現Windows作業系統存在下列安全漏洞，遠端攻擊者可藉由漏洞取得權限或進而執行任意程式碼。行任意程式碼。
 1. 遠端執行任意程式碼漏洞 CVE-2021-36965與CVE-2021-38647
 2. 權限提升漏洞 CVE-2021-36955 CVE-2021-36963 CVE-2021-36968 CVE-2021-38633 CVE-2021-38645 CVE-2021-38648 CVE-2021-38649 CVE-2021-38667 CVE-2021-38671 及 CVE-2021-40447
- 影響平台：
 1. CVE-2021-36955 CVE-2021-36963 CVE-2021-36965 CVE-2021-38633 CVE-2021-38667 CVE-2021-38671 及 CVE-2021-40447
 - 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 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)
2. CVE-2021-38645□CVE-2021-38647□CVE-2021-38648及CVE-2021-38649□\Azure Open Management Infrastructure CVE-2021-36968□
- Windows 7 for 32-bit Systems Service Pack 1
 - Windows 7 for x64-based Systems Service Pack 1
 - 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 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)
- 建議措施：
 - 目前微軟官方已針對此漏洞釋出更新程式，請各機關聯絡維護廠商或參考以下網址進行更新：
 1. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36955>
 2. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36963>
 3. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36965>
 4. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36968>
 5. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38633>
 6. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38645>
 7. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38647>
 8. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38648>
 9. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38649>
 10. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38667>
 11. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38671>
 12. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40447>
 - 參考資料：
 1. <https://www.ithome.com.tw/news/146733>
 2. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36955>
 3. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36963>
 4. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36965>
 5. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36968>
 6. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38633>
 7. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38645>

8. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38647>
 9. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38648>
 10. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38649>
 11. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38667>
 12. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-38671>
 13. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40447>
-

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/mailling:announcement:20210917_02 

Last update: **2021/09/17 15:34**