

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-2020-0105	發布時間	Thu Oct 15 10:27:25 CST 2020
事件類型	漏洞預警	發現時間	Wed Oct 14 00:00:00 CST 2020
警訊名稱	微軟 Windows TCP/IP 堆疊存在安全漏洞(CVE-2020-16898)，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	研究人員發現微軟 Windows TCP/IP 堆疊(TCP/IP stack)未能正確處理 ICMP v6 之路由器公告(Router Advertisement)封包，導致存在安全漏洞(CVE-2020-16898)，遠端攻擊者可藉由發送特製的 ICMPv6 路由器公告封包，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 10 Version 1709 for 32-bit Systems Windows 10 Version 1709 for ARM64-based Systems Windows 10 Version 1709 for x64-based Systems Windows 10 Version 1803 for 32-bit Systems Windows 10 Version 1803 for ARM64-based Systems Windows 10 Version 1803 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 1903 for 32-bit Systems Windows 10 Version 1903 for ARM64-based Systems		

	<p>Windows 10 Version 1903 for x64-based Systems</p> <p>Windows 10 Version 1909 for 32-bit Systems</p> <p>Windows 10 Version 1909 for ARM64-based Systems</p> <p>Windows 10 Version 1909 for x64-based Systems</p> <p>Windows 10 Version 2004 for 32-bit Systems</p> <p>Windows 10 Version 2004 for ARM64-based Systems</p> <p>Windows 10 Version 2004 for x64-based Systems</p> <p>Windows Server 2019</p> <p>Windows Server 2019 (Server Core installation)</p> <p>Windows Server, version 1903 (Server Core installation)</p> <p>Windows Server, version 1909 (Server Core installation)</p> <p>Windows Server, version 2004 (Server Core installation)</p>
影響等級	高
建議措施	<p>1. 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：</p> <p>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898</p> <p>2. 如無法更新，亦可於 Windows 1709 以上版本環境中，執行「netsh int ipv6 set int *INTERFACENUMBER* rbaseddnsconfig=disable」之 PowerShell 指令，藉由停用 ICMPv6 RDNSS 功能，防止攻擊者進行弱點利用。</p>
參考資料	<p>1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898</p> <p>2. https://vuldb.com/?id.162598</p>

此類通告發送對象為通報應變網站登記之資安人員。若貴單位之資安人員有變更，可逕自登入通報應變網站（<https://www.ncert.nat.gov.tw>）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號

聯絡電話： 02-27339922

傳真電話： 02-27331655

電子郵件信箱： service@nccst.nat.gov.tw