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-2020-0006	發布時間	Thu Jan 16 12:01:11 CST 2020
事件類型	漏洞預警	發現時間	Wed Jan 15 00:00:00 CST 2020
警訊名稱	微軟 Windows 作業系統存在安全漏洞(CVE-2020-0601、CVE-2020-0609、CVE-2020-0610 及 CVE-2020-0611)，允許攻擊者進行中間人攻擊或遠端執行任意程式碼，請儘速確認並進行更新		
內容說明	1. 研究人員發現 CryptoAPI(Crypt32.dll)存在安全漏洞(CVE-2020-0601)，遠端攻擊者可利用 CryptoAPI 偽造合法憑證，並以偽造憑證簽署惡意程式，再透過誘騙受害者點擊執行該惡意程式，進而執行任意程式碼，攻擊者亦可利用該漏洞假冒網站或進行中間人攻擊。 2. 研究人員發現遠端桌面閘道(Remote Desktop Gateway)與遠端桌面用戶端程式(Remote Desktop Client)存在安全漏洞(CVE-2020-0609、CVE-2020-0610 及 CVE-2020-0611)，遠端攻擊者可對目標系統之遠端桌面服務發送特製請求，利用此漏洞進而遠端執行任意程式碼。		
影響平台	CVE-2020-0601： ・Microsoft Windows 10 (32、64 位元) ・Microsoft Windows Server 2016 ・Microsoft Windows Server 2019 CVE-2020-0609、CVE-2020-0610： ・Microsoft Windows Server 2012 ・Microsoft Windows Server 2016 ・Microsoft Windows Server 2019 CVE-2020-0611：		

	• Microsoft Windows 7 (32、64 位元) • Microsoft Windows 8.1 (32、64 位元) • Microsoft Windows 10 (32、64 位元) • Microsoft Windows Server 2008 • Microsoft Windows Server 2012 • Microsoft Windows Server 2016 • Microsoft Windows Server 2019
影響等級	高
建議措施	目前微軟官方已針對此弱點釋出更新程式，請儘速進行更新： 1. CVE-2020-0601 之更新已包含在微軟一月份例行性更新中，請至下列連結進行更新： • https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Jan 2. CVE-2020-0609、CVE-2020-0610 及 CVE-2020-0611，請至下列連結進行更新： • https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0609 • https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0610 • https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0611
參考資料	1. https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Jan 2. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0609

	3. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0610 4. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0611 5. https://www.csa.gov.sg/singcert/advisories/advisory-on-critical-vulnerabilities-in-microsoft-windows-operating-system 6. https://thehackernews.com/2020/01/warning-quickly-patch-new-critical.html 7. https://www.ithome.com.tw/news/135366

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