

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-2019-0056 | 發布時間 | Wed May 15 14:00:49 CST 2019 |
| 事件類型 | 漏洞預警 | 發現時間 | Wed May 15 00:00:00 CST 2019 |
| 警訊名稱 | 微軟 Windows 遠端桌面服務存在安全漏洞(CVE-2019-0708)，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 | <p>微軟 Windows 遠端桌面服務(Remote Desktop Services)，在 Windows Server 2008 前之作業系統中稱為終端服務(Terminal Services)，該服務允許使用者透過網路連線進行遠端操作電腦。</p> <p>研究人員發現遠端桌面服務存在安全漏洞(CVE-2019-0708)，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。</p> | | |
| 影響平台 | <p>Windows XP</p> <p>Windows 7</p> <p>Windows Server 2003</p> <p>Windows Server 2008</p> <p>Windows Server 2008 R2</p> | | |
| 影響等級 | 高 | | |
| 建議措施 | <p>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：</p> <p>1.Windows XP 與 Windows Server 2003 作業系統雖已停止支援安全性更新，但微軟仍針對此漏洞釋出更新程式，請至下列連結進行更新：https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708</p> <p>2.作業系統如為 Windows 7、Windows Server 2008 及 Windows Server 2008 R2，請至下列連結進行更新：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708</p> | | |

參考資料

1. <https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/>
2. <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708>

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@ncst.nat.gov.tw