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-2017-0061	發布時間	Fri May 26 10:34:17 CST 2017
事件類型	其他	發現時間	Thu May 25 00:00:00 CST 2017
警訊名稱	特定版本 Samba 軟體存在允許攻擊者遠端執行任意程式碼之漏洞(CVE-2017-7494)，可取得管理者權限，請儘速確認 Samba 軟體版本並進行更新		
內容說明	Samba 是一種用來使 Unix/Linux 作業系統與微軟 Windows 作業系統伺服器訊息區塊(Server Message Block，SMB，又名網路檔案分享系統)協定進行連結的軟體，可運用於共享檔案與網路印表機，以及扮演網域控制站(Domain Controller)角色。 研究人員發現存在超過 7 年之漏洞，該漏洞是 Samba 軟體在處理共享函式庫(share library)時存在問題，導致遠端攻擊者只需扮演具有寫入 Samba 伺服器目錄權限的用戶，並上傳惡意的共享函式庫，伺服器便會載入與執行該共享函式庫，進而在伺服器執行任意程式碼獲得管理者權限。目前 CVE 對此弱點之編號為 CVE 2017-7494。雖尚未傳出實際的案例，但因實現的難度低，且不需使用者介入便可讓攻擊者取得系統權限，因此此弱點又可被視為 Linux 版的 SMB 弱點(例如 WannaCry 所用)，請儘速確認 Samba 軟體版本並進行更新或強化。		
影響平台	Samba 版本大於 3.5.0 與小於 4.4.14/4.5.10/4.6.4		
影響等級	高		
建議措施	1.目前 Samba 官方已針對此弱點釋出修復之版本(https://www.samba.org/samba/history/security.html)，請將 Samba 軟體更新至以下修復之版本，另請密切注意 Samba 官方網頁，以確認是否有相關延伸性之弱點。 ?Samba >= 4.6.4 ?Samba >= 4.5.10 ?Samba >= 4.4.14 2.若現階段無法立即更新 Samba 軟體之版本，則可至 smb.conf 中的[global]		

	區塊添加 nt pipe support = no 參數，以減緩漏洞所造成的影響。 3.透過防火牆或相關防護產品，阻擋來自 Internet 對 Samba 伺服器通訊埠(TCP 445)之連線。
參考資料	1.https://www.samba.org/samba/security/CVE-2017-7494.html 2.http://thehackernews.com/2017/05/samba-rce-exploit.html

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