張貼日期：2017/05/26

[資安漏洞預警通知] 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，可取得管理者權限，請儘速確認Samba軟體版本並進行更新

主旨：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，可取得管理者權限，請儘速確認Samba軟體版本並進行更新

說明：

1. 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。
2. 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。
3. 影響平臺： Samba版本大於3.5.0與小於4.4.14/4.5.10/4.6.4
4. 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。
5. 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

---

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/mailing:announcement:20170526_01

Last update: **2017/05/26 15:09**