OpenSSH 連續被踢爆兩個用戶名稱枚舉漏洞

用戶名稱枚舉漏洞可讓駭客輸入各種用戶名稱，從系統回應判斷用戶名稱的正確性，再以暴力破解找出相對應的密碼，以取得用戶的憑證。

文/陳曉莉 | 2018-08-30 發表

開源的加密通訊專案 OpenSSH 在最近接連被踢爆兩個用戶名稱枚舉 (Username Enumeration) 漏洞，它們分別是 CVE-2018-15473 與 CVE-2018-15919，雖然 OpenSSH 團隊已經修補了前一個漏洞，但他們認為這並不是什麼大不了的漏洞。

SSH 為最市場上最受歡迎的遠端存取協定，可用來執行遠端登入及建立安全通道，而 OpenSSH 即為最普及的 SSH 應用軟體。用戶名稱枚舉漏洞將允許駭客輸入各種用戶名稱，從系統的回應來判斷用戶名稱的正確與否，接著再以暴力破解法找出相對應的密碼，以取得用戶憑證。

其中，CVE-2018-15473 漏洞自 1999 年發表的 OpenSSH 版本就存在了，當駭客送出身分驗證請求時，若所使用的用戶名稱並不存在，

OpenSSH 伺服器即會回覆「驗證失敗」，反之，當確實有該用戶名稱時，OpenSSH 伺服器就會直接關閉連線，這樣的差異將有利於駭客判斷於該伺服器上所註冊的有效用戶名稱。

由於 OpenSSH 廣泛被應用在許多雲端代管伺服器上，也讓資安社群擔心該漏洞將影響數十億的 IoT 裝置。

波蘭資安業者 Securitum 是在今年 7 月提報 CVE-2018-15473，OpenSSH 團隊則已於 7 月底修補，但相關細節一直到 8 月下旬才被披露。

Qualys 則在本周公布了另一個 OpenSSH 用戶名稱枚舉漏洞 CVE-2018-15919，它影響了 2011 年以來的 OpenSSH 版本，此一漏洞存在於 auth2-gss.c 元件中，且在 Fedora、CentOS 及 Red Hat Enterprise Linux 等平台的預設都啟用了該元件。

雖然這兩個漏洞都被分配了漏洞編號，但 OpenSSH 團隊認為它們並沒有那麼嚴重。OpenSSH 開發者 Damien Miller 指出，相關漏洞充其量只能算是「神諭」（Oracle）漏洞，而非枚舉漏洞，因為它們並沒有能力枚舉或列出帳號名單，而只能用暴力破解法來猜測用戶名稱，

再確認這些名稱是否存在於系統上，此外，在 Unix 生態體系中，只有極少數的系統會特意避免這樣的資訊揭露。

不過，Miller 也說若他們知道相關漏洞的存在且修復成本不會太高時，仍會繼續修補這類的漏洞。

資料來源：iThome