張貼日期：2024/07/04

OpenSSH 含有可遠端攻陷伺服器的漏洞 RegreSSHion建議系統管理者儘速評估更新！

主旨：【漏洞預警OpenSSH 含有可遠端攻陷伺服器的漏洞RegreSSHion建議請管理者儘速評估更新！

內容說明：

1. 資安業者Qualys 7/1發布警告，在基於 glibc 之 Linux 系統的 Open Secure Shell(OpenSSH)伺服器上，發現一個安全漏洞 CVE-2024-6387該漏洞將允許未經授權的駭客自遠端執行任意程式，該漏洞影響絕大多數的 Linux 版本。
2. OpenSSH 團隊亦於該日發布了 OpenSSH 9.8/9.8p1 版本，修補本次 CVE-2024-6387 高風險漏洞，解決允許駭客在不需要身分驗證的情況下，自遠端執行任意程式，還能以最高權限執行之狀況。
3. OpenBSD 不會受本次漏洞所影響。

影響平台：
linux

漏洞影響版本：

- 8.5p1 ≤ OpenSSH < 9.8p1 之間的版本。
- OpenSSH < 4.4p1 版本（如果該版本未針對 CVE-2006-5051 或 CVE-2008-4109 進行修補）。

建議措施：
請參考各 linux 發行版官方公告資訊，進行更新修補。

參考資料:
https://www.qualys.com/regresshion-cve-2024-6387/
https://www.cve.org/CVERecord?id=CVE-2024-6387
https://www.openssh.com/txt/release-9.8
https://www.ithome.com.tw/news/163737

計算機與通訊中心
網路系統組 敬啟