張貼日期：2023/08/09

【漏洞預警□OpenSSH存在高風險安全漏洞(CVE-2023-38408)□允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新或評估採取緩解措施！

- 主旨說明：轉發 國家資安資訊分享與分析中心 NISAC-200-202308-00000012□

研究人員發現OpenSSH之金鑰暫存元件ssh-agent存在不帶引號搜尋路徑(Unquoted Search Path)漏洞(CVE-2023-38408)□允許攻擊者透過SSH金鑰轉發機制，利用此漏洞達到遠端執行任意程式碼。

- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-200-202308-00000012□
  - 研究人員發現OpenSSH之金鑰暫存元件ssh-agent存在不帶引號搜尋路徑(Unquoted Search Path)漏洞(CVE-2023-38408)□允許攻擊者透過SSH金鑰轉發機制，利用此漏洞達到遠端執行任意程式碼。
- 影響平台:
  - OpenSSH 5.5至9.3p1版本
- 建議措施:
  - 請升級至OpenSSH 9.3p2(含)以上版本。
    1. 根據作業系統不同，可參考下列指令更新：
       1. Ubuntu與Debian apt-get update apt-get upgrade openssh
       2. CentOS□RHEL□Fedora及OpenSUSE yum update openssh -y
    2. 可參考以下網址下載更新檔並進行手動安裝 https://www.openssh.com/portable.html
- 參考資料:
  1. https://www.openssh.com/portable.html
  2. https://nvd.nist.gov/vuln/detail/CVE-2023-38408

計算機與通訊中心
網路系統組 敬啟