CVE vulnerability

Introduction

- 這個缺陷會導致curl在SOCKS5代理握手過程中使一個基於堆的緩衝區發生溢出。當curl被請求將主機名傳遞給SOCKS5代理，以便代理解析地址，而不是由curl自身完成時，該主機名的最大長度可為255字節。如果檢測到主機名長度超過此限制，curl將切換到本地名稱解析，並只傳遞解析後的地址。由於這個錯誤，表示“讓主機解析名稱”的本地變量在一個慢速的SOCKS5握手過程中可能獲得錯誤的值，與預期相反，它將太長的主機名複製到目標緩衝區，而不是僅將解析後的地址複製到那裡。目標緩衝區是一個基於堆的緩衝區，而主機名來自curl被告知操作的URL。

CVE environment

- 為了重現這個漏洞,我需要傳遞主機名至socks5,我選擇連接至 9050 端口配置代理,此外,由於版本太高會導致無法重現漏洞,所以 curl 我選擇使用8.1.2
- 後來發現8.3.0也可以,新連接socks5時使用的版本為curl 8.3.0

Reproduce exploitation

- 首先我採用limit rate的方式限制流量,如果流量超過所設定值,便會溢出進到緩衝區,由此觀測是否會指傳遞解析後的位置,並獲得錯誤的值,並且採取了tee命令以獲取觀測日誌去觀察輸出尋找安全漏洞的跡象,而curl中也有自動生成命令的紀錄,紀載有關可能程序崩潰之類的紀錄,後來改為使用danted.server之log直接讓發生溢出之cause寫入裡面.

Reproduce exploitation implement

- 首先要安裝socks5代理服務器danted server,這樣才能使用各項授權功能,包含更改配置文件以及服務,接著去danted config修改enp0s3為你的虛擬機上之乙太網路接口

Reproduce exploitation implement(2)

- 去socks5服務器上開啟socks5服務,接著啟動已經預寫好之server.py(已附加在檔案中)
- 利用curl -v --limit-rate 256 --proxy socks5h://192.168.1.1:10808 -L http://192.168.1.1:8000指令執行payload,會復原此漏洞所形成之超過主機長枝自節複製到緩衝區