B09902063　資工二 董瑋

Summary:

2020 年末由臺灣資安公司戴夫寇爾發現在微軟 Exchange server 上的重大安全性漏洞(ProxyLogon)，利用這個漏洞駭客可以將 webshell 後門程式安裝在伺服器上用以竊取機密文件，這次的核心漏洞則是未經身分驗證的 SSRF 漏洞，駭客可以透過這個漏洞繞過身分驗證到達伺服器達到 RCE 的目的。這次漏洞的受害者甚多，在漏洞被披露後，全世界範圍內有超過數十萬部伺服器遭惡意攻擊，而這次作為攻擊對象的 exchange server 所扮演的角色也是極其重要，它所掌握的企業的 email 中包含了許許多多的機密文件。以台灣遭受攻擊的企業為例，筆電代工大廠廣達就因這個漏洞被駭客竊走 Apple 交付給他們的 Mac 設計圖，因不願交付贖金使得現在就能在暗網上找到未上市的 Mac 設計圖，也因此讓廣達的商譽受到影響。

Impact or implications on security

ProxyLogon 不同於以往常見的記憶體毀損類型的漏洞，它是在程式設計上的邏輯漏洞，這同時也是一個全新的攻擊面向。許多安全研究員和駭客也已經開始挖掘漏洞，試圖在對方發現前做出最大的努力，現在也已經有許多漏洞被發現，如 ProxyShell 和 ProxyToken 都是最近才被發現且十分嚴重的安全性漏洞。值得注意的是，美國司法部也授權 FBI 主動替被安裝惡意 webshell 的用戶移除掉這些惡意程式，雖然沒有幫這些用戶補上漏洞，但這也顯現出這次漏洞的嚴重性和範圍之廣。

My reflection

這次的漏洞影響的層面十分之廣，因為 exchange server 不單單是學術界在使用，許多企業也會用以傳輸機密文件。這也顯示出做為一名程式設計師，我們必須對自己所寫出來的東西有點責任心，否則若寫出含有邏輯漏洞的 code 就會被有心人士利用。這次被駭的多是向企業勒索贖金，倘若這次被駭的是一些基礎硬體設施像火災警報、紅綠燈信號、電力控制系統等等，這就不單單只是金錢上的損失，更可能有人因此喪命。因此做為一位資訊系的學生，我應該學著開始審慎面對自己寫出來的東西在某些情況下是否會有些致命的邏輯漏洞，並且試著去修復它。

Ref

https://www.ithome.com.tw/news/143819

https://www.cc.ntu.edu.tw/chinese/epaper/0057/20210620_5706.html

https://www.bnext.com.tw/article/62421/revil-quanta-hacker-macbook-air-leak

https://devco.re/blog/2021/08/07/a-new-attack-surface-on-MS-exchange/

https://udn.com/news/story/7240/5404993