CVE-2023-35936 發現以及 0-day

專題編號：112-CSIE-S020
執行期限：111 年第 1 學期至 112 年第 1 學期
指導教授：陳彥霖 教授
專題參與人員： 108810039 張洸銘

一、摘要

關鍵詞： Arbitrary Read File, Arbitrary Write File, Remote Code Execution(Pre Auth)

有一位睿智的駭客曾經說過，自己用的服務自己打，剛好在 DEVCORE 實習期間用了一個 HackMD 公司所開發的開源軟體 CodiMD 來架設大家筆記的軟體，在使用之後發現一些服務出現了一些問題，使用了 Pre Auth 可以寫檔案的 API 加上 Arbitrary Write File，更是發現了一條不用登入也可以造成 Remote Code Execution 的嚴重漏洞。

二、緣由與目的

有一位睿智的駭客曾經說過，自己用的服務自己打，沒有打過自己所使用服務的駭客怎麼能算真正的駭客呢，在如此的契機之下開始挖掘了在 DEVCORE 實習期間使用的開源筆記軟體 CodiMD，在裡面所提供的服務發現有一些不對的地方。透過此次研究，當然是希望可以找到一條可以輕鬆達到 Remote Code Execution 的路徑。

三、研究範圍

為了找到一條可以輕鬆達到 Pre Auth Remote Code Execution 的路徑，需要不僅僅只是 CodiMD 的開源程式碼，還需要他所使用來轉檔的軟體 Pandoc 的開源程式碼來研究，在研究的過程中發現 Pandoc 的官方文檔中已經說明了在轉檔案使用的格式存在任意讀取檔案的問題，也給出了應對的方式，但是在 CodiMD 的原始碼中看不到這些防範以及沒有指定格式導致可以任意指定，這些問題也是導致造成任意程式碼執行的主因。

四、使用技術

基本上先透過黑箱測試鎖定有問題的服務，再透過 GitHub 找到對應服務的開源程式碼並且透過人工查閱程式碼的方式看到問題的成因，再查閱相關文檔發現已經有的警告，在實作的過程中發現 CodiMD 確實沒有注意到這些問題，因此可以達成任意讀取檔案。

在接下來研究文檔中提及到的文件格式發現其中一個格式會使用 pdflatex 來跑 latex 的程式碼，因此透過一些 Race Condition 的方法可以在寫檔案的間隙讀取該檔案造成任意程式碼執行，但是由於

這個方式需要機器下載 pdflatex 而不是在 default environment 下可以造成的結果，因此從 pandoc 本身找 0-day。

在黑箱研究 pandoc 的時候發現其中一個格式的檔案會存指定的圖片路徑，因此可以透過指定圖片路徑來達到任意檔案存取，再經過讀取該檔案達到任意程式碼執行，又 CodiMD 開發了一個 API 可以讓沒有登入的使用者寫任意筆記，只要有讀取的權限，因此可以輕鬆地達到 Pre Auth Remote Code Execution。

五、結論

此次研究揭示了 CodiMD 和 Pandoc 開源軟體中的多個嚴重漏洞，這些漏洞可能導致未經授權的檔案訪問和任意程式碼執行。這不僅損害了數據完整性，還可能對系統安全性和機密性構成重大風險。因此，我們建議軟體開發者應加強對安全性的考慮，定期進行漏洞掃描和修復，以確保使用者的資料和系統得到妥善保護。

這項研究也強調了駭客和安全研究人員在發現和報告潛在漏洞時的關鍵作用。透過此類研究，我們可以更好地了解潛在威脅，幫助開發者改進他們的軟體，以確保安全性和可靠性。在未來，我們應該持續關注安全性，並致力於共同保護數位世界的資訊和資產。

參考文獻

[1] *Pandoc - index*. (n.d.). https://pandoc.org/

[2] *CODiMD Documentation - HackMD*. (n.d.). HackMD. https://hackmd.io/c/codimd-documentation/%2Fs%2Fcodimd-documentation