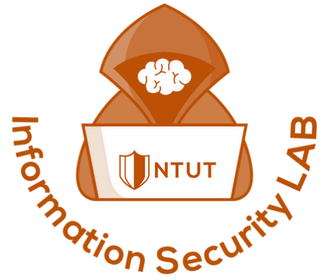
APACHE 2.4.49



CVE-2021-41773

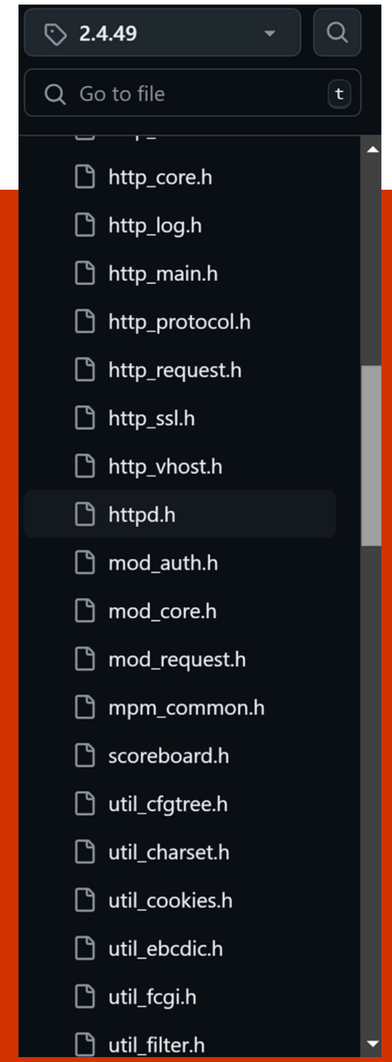
漏洞復現

Apache HTTP Server

1. 是一個由多個模組建構起來的系統
2. 官方所列出的 136 個模組其中約有

   快一半是預設啟用或經常被使用的模組
3. 多模組彼此之間共同維護著 request_rec 結構

   這個結構包括了在處理 HTTP 時會用到的一切元素



官方文件：https://httpd.apache.org/docs/2.4/mpm.html
官方列出模組：https://github.com/apache/httpd/blob/2.4.49/include/httpd.h#L1780

CVE-2021-41773

What’s going on?

版本 2.4.49 函數 ap_normalize_path() 會過濾

./ 或是 ../ ，但如果改成 16進制 EX：.%2e/ 或 %2e%2e/

就可以達成 Path Traversal，如果有啟用 cgi 或 cgid 模組

則可以達成 RCE

Apache HTTP Server

what 2.4.49 actually do ?

```
560                 if (path[l] == '.') {
561                     /* Remove /./ segments */
562                     if (IS_SLASH_OR_NUL(path[l + 1])) {
563                         l++;
564                         if (path[l]) {
565                             l++;
566                         }
567                         continue;
568                     }
569
570                     /* Remove /xx/../ segments */
571                     if (path[l + 1] == '.' && IS_SLASH_OR_NUL(path[l + 2])) {
572                         /* Wind w back to remove the previous segment */
573                         if (w > 1) {
574                             do {
575                                 w--;
576                             } while (w && !IS_SLASH(path[w - 1]));
577                         }
578                         else {
579                             /* Already at root, ignore and return a failure
580                              * if asked to.
581                              */
582                             if (flags & AP_NORMALIZE_NOT_ABOVE_ROOT) {
583                                 ret = 0;
584                             }
585                         }
```

What's build it up?

httpd.conf

預設之下是允許訪問目錄，或是直接配置

<Directory /> Require all granted </Directory>

```
<Directory />
    AllowOverride none

    #here is important:

     #Require all denied
</Directory>
```

What's build it up?

CGI OR CGID

啟用後可以利用 /bin/sh 達到 RCE

```
"s|#LoadModule cgid_module modules/mod_cgid.so|LoadModule cgid_module modules/
 /usr/local/apache2/conf/httpd.conf \
"s|#LoadModule cgi_module modules/mod_cgi.so|LoadModule cgi_module modules/
/usr/local/apache2/conf/httpd.conf \
```

What's build it up?

Dockerfile

Open | Dockerfile ~/Desktop/CVE-41773/test1 | Save

```
1  FROM httpd:2.4.49
2
3  RUN set -ex \
4      && sed -i "s|#LoadModule cgid_module modules/mod_cgid.so|LoadModule cgid_module modules/mod_cgid.so|g" /usr/local/apache2/conf/httpd.conf \
5      && sed -i "s|#LoadModule cgi_module modules/mod_cgi.so|LoadModule cgi_module modules/mod_cgi.so|g" /usr/local/apache2/conf/httpd.conf \
6      && sed -i "s|#Include conf/extra/httpd-autoindex.conf|Include conf/extra/httpd-autoindex.conf|g" /usr/local/apache2/conf/httpd.conf \
7      && cat /usr/local/apache2/conf/httpd.conf \
8          | tr '\n' '\r' \
9          | perl -pe 's|<Directory />.*?</Directory>|<Directory />\n    AllowOverride none\n    Require all granted\n</Directory>|isg' \
10         | tr '\r' '\n' \
11         | tee /tmp/httpd.conf \
12     && mv /tmp/httpd.conf /usr/local/apache2/conf/httpd.conf
```

DEMO

CVE-2021-41773

如何修補這個漏洞

這個漏洞影響了2.4.49 以及 2.4.50 (CVE-2021-42013)

修補方法：更新到最新版本

CVE-2021-41773

如何修補這個漏洞

這個漏洞影響了2.4.49 以及 2.4.50 (CVE-2021-42013)

修補方法：更新到最新版本

他做了甚麼修補???

APACHE 2.4.50

CVE-2021-42013

漏洞復現

Apache HTTP Server

what 2.4.50 actually do ?

```
561                 if (path[l] == '.') {
562                     /* Remove /./ segments */
563                     if (IS_SLASH_OR_NUL(path[l + 1])) {
564                         l++;
565                         if (path[l]) {
566                             l++;
567                         }
568                         continue;
569                     }
570
571                     /* Remove /xx/../ segments (or /xx/.%2e/ when
572                      * AP_NORMALIZE_DECODE_UNRESERVED is set since we
573                      * decoded only the first dot above).
574                      */
575                     n = l + 1;
576                     if ((path[n] == '.' || (decode_unreserved
577                                             && path[n] == '%'
578                                             && path[++n] == '2'
579                                             && (path[++n] == 'e'
580                                                 || path[n] == 'E')))
581                             && IS_SLASH_OR_NUL(path[n + 1])) {
```

CVE-2021-41773

What’s going on?

版本 2.4.50 函數同上一個版本 ，只是因為他還多將 %2e 過濾掉了，所以只要將 %2e 再拿去轉成 ASCII 就好了 EX：

%%32%65/ 或 %%32%65%%32%65/

CVE-2021-41773

What's going on?

%%32%65/ 或 %%32%65%%32%65/

%2e/ 或 %2e%2e/

./ 或 ../

DEMO

CVE-2021-42013

如何修補這個漏洞

修補方法：更新到最新版本

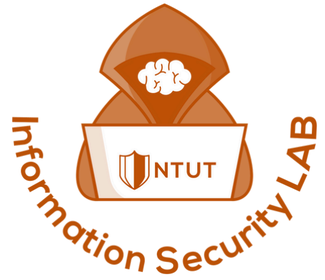
下一個版本 2.4.51

引入 ap_unescape_url_ex() 去控制 url decode

並且棄用了沒在使用的

AP_NORMALIZE_DROP_PARAMETERS flag

APACHE 2.4.49



THANK YOU