Sample Penetration Test Report

Example Company

Company: Customer Name
Date: 06 July 2024
Version 1.0

Pendahuluan

CVE-2021-42013 dan CVE-2021-41773 adalah kerentanan keamanan yang ditemukan pada Apache HTTP Server. Kedua kerentanan ini berkaitan dengan Path Traversal dan Remote Code Execution (RCE), yang memungkinkan penyerang untuk mengakses file sistem yang seharusnya tidak dapat diakses atau menjalankan kode berbahaya di server yang rentan.

- CVE-2021-41773 ditemukan terlebih dahulu dan dilaporkan pada awal Oktober 2021. Kerentanan ini memungkinkan penyerang untuk melakukan path traversal pada konfigurasi tertentu dari Apache HTTP Server, sehingga memungkinkan akses ke file yang tidak dimaksudkan untuk diakses oleh publik.

- CVE-2021-42013 adalah pembaruan dari CVE-2021-41773 yang dirilis setelah ditemukan bahwa patch awal tidak sepenuhnya mengatasi masalah. CVE-2021-42013 memungkinkan penyerang untuk melakukan remote code execution (RCE) selain path traversal.

Metodologi Penyerangan

Metodologi penyerangan untuk kedua kerentanan ini melibatkan beberapa langkah:

- Path Traversal: Penyerang dapat menggunakan urutan direktori ".." (dot-dot) dalam URL (URL Manipulation) untuk menavigasi keluar dari direktori root yang ditentukan oleh server web dan mengakses file di luar root tersebut. Misalnya, dengan mengirimkan permintaan HTTP seperti `http://{target_ip}:{port}/cgi-bin/../../../../etc/passwd`, penyerang dapat mengakses file `passwd` yang berisi informasi akun pengguna.

- Remote Code Execution (RCE): Pada CVE-2021-42013, selain melakukan path traversal, penyerang juga dapat menyisipkan payload berbahaya yang memungkinkan eksekusi kode di server yang rentan. Ini dilakukan dengan mengirimkan permintaan HTTP yang memanfaatkan cgi-bin atau modul serupa yang diekspos oleh server.

Identifikasi Kerentanan

Identifikasi kerentanan ini melibatkan beberapa langkah teknis:

- Analisis Konfigurasi Server: Pemeriksaan konfigurasi Apache HTTP Server untuk menemukan pengaturan yang memungkinkan path traversal. Ini termasuk memeriksa apakah mod_cgi atau modul serupa diaktifkan dan dikonfigurasi dengan benar.

- Pengujian Path Traversal: Mengirimkan permintaan HTTP dengan pola ".." untuk menguji apakah server memungkinkan akses ke file yang tidak seharusnya diakses. Contoh permintaan bisa berupa `GET /cgi-bin/../../../../etc/passwd HTTP/1.1`.

- Eksploitasi RCE: Mengirimkan payload yang dirancang untuk menguji apakah server rentan terhadap eksekusi kode jarak jauh.

- Log Analisis: Memeriksa log server untuk tanda-tanda eksploitasi, seperti permintaan yang mencurigakan atau akses yang tidak sah ke file sistem.

Hasil pemindaian Nmap

Starting Nmap 7.94 (https://nmap.org) at 2024-07-06 16:04 SE Asia Standard Time

Nmap scan report for 152.42.212.132

Host is up (0.031s latency).

PORT STATE SERVICE VERSION

889/tcp open http Apache httpd 2.4.50 ((Unix))

|_http-title: Site doesn't have a title (text/html).

| http-methods:

|_ Potentially risky methods: TRACE

|_http-server-header: Apache/2.4.50 (Unix)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 35.52 seconds

Pemindaian Kerentanan dan Eksploitasi

http://152.42.212.132:889 is vulnerable to Path Traversal Attack (CVE-2021-42013)

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

_apt:x:100:65534::/nonexistent:/usr/sbin/nologin

http://152.42.212.132:889 is vulnerable to Remote Code Execution attack (CVE-2021-42013)

uid=1(daemon) gid=1(daemon) groups=1(daemon)

[+] whoami:

[+] ls:

[+] pwd:

[+] uname -a:

Rekomendasi dan Mitigasi

Rekomendasi dan mitigasi berikut dapat membantu dalam mengamankan Apache HTTP Server dari kerentanan yang terkait dengan CVE-2021-42013 dan CVE-2021-41773:

Rekomendasi

1. Pembaruan dan Patching:

- Segera Perbarui Apache HTTP Server: Versi yang terdampak dari Apache HTTP Server adalah 2.4.49 dan 2.4.50. Disarankan untuk segera memperbarui ke versi 2.4.51 atau lebih baru, yang telah memperbaiki kerentanan ini.

2. Konfigurasi Server yang Aman:

- Nonaktifkan CGI jika Tidak Diperlukan: Jika mod_cgi atau modul CGI serupa tidak diperlukan, sebaiknya nonaktifkan modul tersebut untuk mengurangi permukaan serangan.

- Periksa dan Atur Konfigurasi Directory: Pastikan konfigurasi direktori server tidak memungkinkan akses ke direktori di luar root yang diizinkan. Misalnya, gunakan pengaturan `Options -Indexes` dan `Require all denied` di konfigurasi Apache untuk membatasi akses.

- Gunakan `Alias` atau `ScriptAlias`: Gunakan instruksi `Alias` atau `ScriptAlias` dengan hati-hati untuk memastikan bahwa hanya direktori yang ditentukan yang dapat diakses melalui URL.

3. Penggunaan Firewall dan IDS/IPS:

- WAF (Web Application Firewall): Gunakan WAF untuk mendeteksi dan mencegah serangan path traversal dan RCE. Banyak WAF modern dapat mengidentifikasi pola serangan yang diketahui dan memblokirnya sebelum mencapai server web.

- IDS/IPS (Intrusion Detection/Prevention Systems): Implementasikan IDS/IPS untuk memantau lalu lintas jaringan dan mendeteksi tanda-tanda eksploitasi kerentanan.

Mitigasi

1. Pengamanan Akses File:

- Isolasi Direktori Penting: Pastikan file dan direktori yang sensitif, seperti `/etc/passwd`, tidak dapat diakses melalui web server dengan cara apapun. Gunakan izin file yang ketat dan kontrol akses yang sesuai.

2. Pengetesan Keamanan Rutin:

- Penetration Testing: Lakukan pengujian penetrasi secara rutin untuk mengidentifikasi dan mengatasi kerentanan baru yang mungkin muncul. Pastikan pengujian mencakup upaya eksploitasi path traversal dan RCE.

- Code Review: Lakukan review kode aplikasi web secara rutin untuk mengidentifikasi dan memperbaiki kerentanan keamanan, terutama pada modul-modul yang dapat diakses melalui web.

3. Monitoring dan Respons Insiden:

- Log Monitoring: Pantau log server web untuk mendeteksi aktivitas mencurigakan yang mungkin menandakan upaya eksploitasi. Gunakan alat monitoring log yang dapat memberi tahu tim keamanan secara real-time.

- Incident Response Plan: Siapkan rencana respons insiden untuk menghadapi eksploitasi yang berhasil. Rencana ini harus mencakup isolasi server yang terdampak, analisis forensik, dan langkah-langkah mitigasi.

Contoh Konfigurasi Apache untuk Mitigasi

Berikut adalah contoh konfigurasi yang dapat digunakan untuk mengurangi risiko eksploitasi path traversal dan RCE:

```apache

# Nonaktifkan direktori listing
```

Options -Indexes

Batasi akses ke direktori tertentu

AllowOverride None

Require all denied

Konfigurasi CGI dengan aman

AllowOverride None

Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch

Require all granted

Blokir pola path traversal

Require all denied

```

Dengan mengikuti rekomendasi dan mitigasi ini, risiko yang terkait dengan CVE-2021-42013 dan CVE-2021-41773 dapat diminimalkan, memastikan bahwa server Apache HTTP Anda tetap aman dari eksploitasi yang mungkin terjadi.
```