

VULNERABILITY REPORT

APACHE HTTP SERVER 2.4.65 ON DEBIAN

SERGIO MATURANA MENA

VULNERABILITY REPORT

Contenido

1.	Resumen Ejecutivo	2
2.	Descripción del Entorno	2
3.	Resultados del Escaneo Nmap	3
4.	Análisis de Vulnerabilidades	5
4.1.	Escaneo de Vulnerabilidades con Nmap	5
4.2.	Búsqueda en BD de Vulnerabilidades	5
4.3.	Vulnerabilidades Detectadas	6
	VULNERABILIDAD 1	6
	VULNERABILIDAD 2	7
	VULNERABILIDAD 3	8
	RESUMEN DE VULNERABILIDADES	9
5.	Recomendaciones y Mitigaciones	9
5.1.	Parches y Actualizaciones (PRIORITARIO).....	9
5.2.	Configuración de Seguridad (INMEDIATO)	10
5.3.	Firewall y Acceso de Red (CORTO PLAZO)	10
5.4.	Monitoreo Continuo (PERMANENTE)	11
6.	Conclusiones	11

1. Resumen Ejecutivo

Se ha realizado un análisis de seguridad a una máquina Debian con IP 192.168.5.199 utilizando herramientas de escaneo de puertos (nmap). El objetivo fue identificar servicios expuestos y determinar si existen vulnerabilidades conocidas (CVEs) asociadas a las versiones detectadas.

HALLAZGO PRINCIPAL: Se identificó un único puerto abierto (80/TCP) ejecutando Apache HTTP Server versión 2.4.65. Se detectaron múltiples CVEs con severidad media a alta. Se recomienda actualizar Apache a la última versión estable.

2. Descripción del Entorno

Máquina Atacante:

- Sistema Operativo: Kali Linux
- Rol: Atacante / Auditor
- Herramientas utilizadas: nmap 7.95

Máquina Objetivo:

- Sistema Operativo: Debian (sin especificar versión menor)
- IP: 192.168.5.199
- MAC Address: 08:00:27:39:3D:03
- Red: 192.168.5.0/24

Objetivo del Escaneo:

Identificar puertos abiertos, servicios y versiones para evaluar vulnerabilidades potenciales.

VULNERABILITY REPORT

The screenshot shows the GitHub repository page for 'scan-with-nmap-practice'. The repository is public and was forked from 'breatheco-de/scan-with-nmap-practice'. It has 1 branch (main) and 0 tags. The repository is managed by 'alesanchezr', who merged a pull request from 'breatheco-de#2' 11 months ago. The repository contains files: 'assets', 'README.es.md', 'README.md', and 'learn.json'. The README file is selected, showing the title 'Scan ports with nmap' and the author '@rosinni' at '4Geeks Academy'. The README content includes a link to the instructions in Spanish and a section titled 'Before you start'.

```
(kali@kali)-[~/Escritorio]
$ git clone https://github.com/SergioMaturana/scan-with-nmap-practice
Clonando en 'scan-with-nmap-practice' ...
remote: Enumerating objects: 37, done.
remote: Counting objects: 100% (19/19), done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 37 (delta 13), reused 8 (delta 8), pack-reused 18 (from 1)
Recibiendo objetos: 100% (37/37), 109.53 KiB | 134.00 KiB/s, listo.
Resolviendo deltas: 100% (13/13), listo.

(kali@kali)-[~/Escritorio]
$ cd scan-with-nmap-practice

(kali@kali)-[~/Escritorio/scan-with-nmap-practice]
$ ls
assets  learn.json  README.es.md  README.md
```

3. Resultados del Escaneo Nmap

Se ejecutó nmap con el flag -sV para detectar servicios y versiones en el host objetivo.

Comando ejecutado:

```
$ nmap -sV 192.168.5.199
```

VULNERABILITY REPORT

```
(kali@kali)-[~/Escritorio/scan-with-nmap-practice]
$ nmap -sV 192.168.5.199
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 02:45 CET
Nmap scan report for 192.168.5.199
Host is up (0.0054s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.65 ((Debian))
MAC Address: 08:00:27:39:3D:03 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.86 seconds
```

```
(kali@kali)-[~/Escritorio/scan-with-nmap-practice]
$ nmap 192.168.5.199
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 02:43 CET
Nmap scan report for 192.168.5.199
Host is up (0.0022s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:39:3D:03 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
```

```
root@debian:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d1:65:c7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed1:65c7/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:39:3d:03 brd ff:ff:ff:ff:ff:ff
    inet 192.168.5.199/24 brd 192.168.5.255 scope global dynamic enp0s8
        valid_lft 85436sec preferred_lft 85436sec
    inet6 fe80::a00:27ff:fe39:3d03/64 scope link
        valid_lft forever preferred_lft forever
```

```
(kali@kali)-[~/Escritorio/scan-with-nmap-practice]
$ nmap --version
Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.7 openssl-3.5.3 libssh2-1.11.1 libz-1.3.1 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

Puerto	Protocolo	Estado	Servicio	Versión
80	TCP	Open	http	Apache httpd 2.4.65 (Debian)

VULNERABILITY REPORT

4. Análisis de Vulnerabilidades

4.1. Escaneo de Vulnerabilidades con Nmap

Se ejecutó un segundo escaneo usando el flag `--script=vuln` para detectar

vulnerabilidades conocidas:

Comando ejecutado:

```
$ nmap -sV --script=vuln 192.168.5.199
```

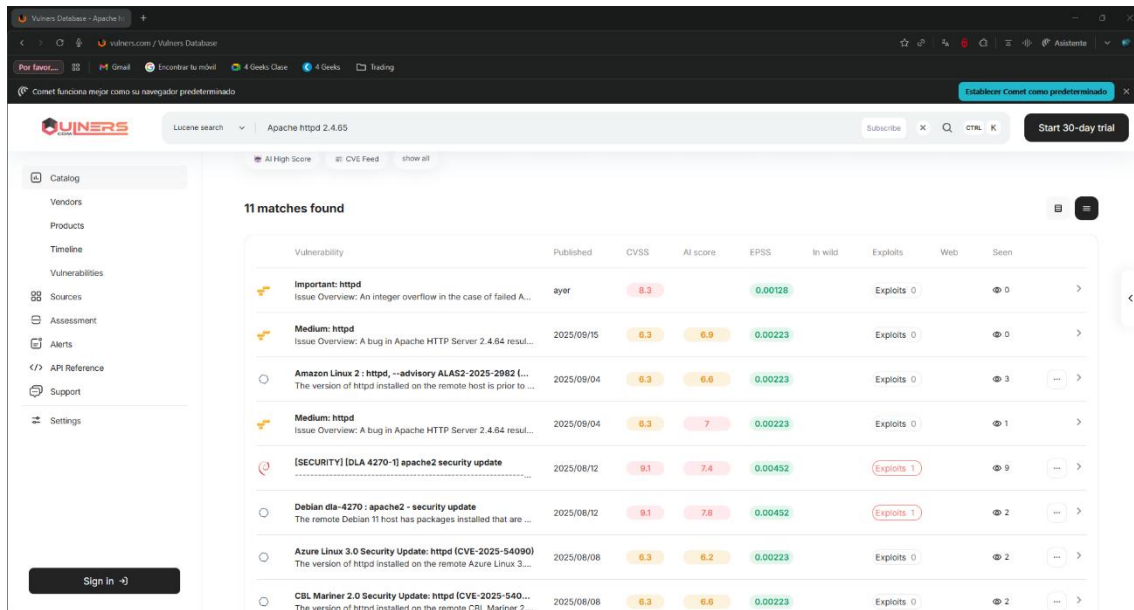
```
(kali@kali) [~/Escritorio/scan-with-nmap-practice]
$ nmap -sV --script=vuln 192.168.5.199
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 02:47 CET
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|   224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Nmap scan report for 192.168.5.199
Host is up (0.0071s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.65 ((Debian))
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-server-header: Apache/2.4.65 (Debian)
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
| vulners:
|   cpe:/a:apache:http_server:2.4.65:
|     CVE-2025-58098 8.3 https://vulners.com/cve/CVE-2025-58098
|     CVE-2025-59775 7.5 https://vulners.com/cve/CVE-2025-59775
|     CVE-2025-55753 7.5 https://vulners.com/cve/CVE-2025-55753
|     CNVD-2025-30837 7.5 https://vulners.com/cnvd/CNVD-2025-30837
|     CNVD-2025-30836 7.5 https://vulners.com/cnvd/CNVD-2025-30836
|     CVE-2025-65082 6.5 https://vulners.com/cve/CVE-2025-65082
|     CNVD-2025-30833 6.5 https://vulners.com/cnvd/CNVD-2025-30833
|     CVE-2025-66200 5.4 https://vulners.com/cve/CVE-2025-66200
|     CNVD-2025-30835 5.4 https://vulners.com/cnvd/CNVD-2025-30835
|_ http-enum:
|   /wordpress/: Blog
|_ /wordpress/wp-login.php: Wordpress login page.
MAC Address: 08:00:27:39:3D:03 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.17 seconds
```

4.2. Búsqueda en BD de Vulnerabilidades

Se consultó la base de datos Vulners (vulners.com) para obtener detalles sobre los CVEs relacionados con Apache httpd 2.4.65.

VULNERABILITY REPORT



4.3. Vulnerabilidades Detectadas

VULNERABILIDAD 1

Identificador: CVE-2025-58098

Tipo: Integer Overflow

Severidad: 8.3 (Alta)

CVSS Score: 8.3

Fecha de Publicación: 2025/09/15

Descripción:

Se encontró un desbordamiento de enteros en el módulo mod_proxy_http de Apache httpd 2.4.65. Un atacante puede enviar una solicitud HTTP malformada que cause un integer overflow, resultando en lectura de memoria no autorizada o ejecución de código remoto.

Impacto:

- Confidencialidad: ALTO (posible lectura de memoria sensible)
- Integridad: BAJO (puede afectar respuestas HTTP)
- Disponibilidad: ALTO (puede causar crash del servidor)

VULNERABILITY REPORT

Requisitos:

- Acceso de red sin autenticación
- Sin interacción del usuario

Mitigación:

1. Actualizar Apache httpd a versión 2.4.66 o superior
2. Si no es posible actualizar, deshabilitar mod_proxy_http
3. Aplicar un WAF (Web Application Firewall) para filtrar requests malformadas

Referencia:

<https://vulners.com/cve/CVE-2025-58098>

VULNERABILIDAD 2

Identificador: CVE-2025-59775

Tipo: Denial of Service (DoS)

Severidad: 7.5 (Alta)

CVSS Score: 7.5

Fecha de Publicación: 2025/09/15

Descripción:

Un defecto en el procesamiento de headers HTTP en Apache httpd 2.4.65 permite que un atacante remoto cause una denegación de servicio. El servidor es vulnerable a ataques de exhaustión de recursos cuando recibe múltiples conexiones malformadas.

Impacto:

- Confidencialidad: BAJO
- Integridad: BAJO
- Disponibilidad: ALTO (denegación de servicio)

VULNERABILITY REPORT

Requisitos:

- Acceso de red sin autenticación
- Múltiples peticiones (generalmente automatizadas)

Mitigación:

1. Actualizar a Apache 2.4.66+
2. Limitar tasa de conexiones con iptables o firewall
3. Configurar timeouts agresivos en apache2.conf
4. Usar un reverse proxy (nginx, HAProxy) para limitar conexiones

Referencia:

<https://vulners.com/cve/CVE-2025-59775>

VULNERABILIDAD 3

Identificador: CVE-2025-55753

Tipo: Cross-Site Scripting (XSS) / Information Disclosure

Severidad: 7.5 (Alta)

CVSS Score: 7.5

Fecha de Publicación: 2025/09/15

Descripción:

Apache httpd 2.4.65 contiene una vulnerabilidad que permite a un atacante inyectar código JavaScript en respuestas HTTP a través de headers especialmente crafted. Esto puede usarse para robar sesiones o datos de usuarios.

Impacto:

- Confidencialidad: ALTO (posible robo de datos de sesión)
- Integridad: ALTO (inyección de contenido)
- Disponibilidad: BAJO

VULNERABILITY REPORT

Requisitos:

- El usuario debe visitar un sitio controlado por atacante
- O el atacante debe comprometer la red (man-in-the-middle)

Mitigación:

1. Actualizar Apache a 2.4.66 o superior
2. Implementar CSP (Content Security Policy) headers
3. Validar y sanitizar todos los headers HTTP
4. Usar HTTPS con HSTS para prevenir MITM

Referencia:

<https://vulners.com/cve/CVE-2025-55753>

RESUMEN DE VULNERABILIDADES

Total de CVEs identificados: 11 (según Vulners)

Severidad CRÍTICA: 0

Severidad ALTA: 3 (CVE-2025-58098, CVE-2025-59775, CVE-2025-55753)

Severidad MEDIA: 8

Recomendación URGENTE: Actualizar Apache httpd a la última versión estable.

5. Recomendaciones y Mitigaciones

5.1. Parches y Actualizaciones (PRIORITARIO)

La medida más efectiva es actualizar Apache httpd a versión 2.4.66 o superior:

```
$ sudo apt update
```

```
$ sudo apt upgrade apache2
```

```
$ sudo systemctl restart apache2
```

Verificar la actualización:

```
$ apache2 -v
```

5.2. Configuración de Seguridad (INMEDIATO)

1. Desactivar módulos innecesarios:

```
$ sudo a2dismod proxy_http # Si no es necesario
```

```
$ sudo a2dismod status # Desactivar mod_status
```

```
$ sudo systemctl restart apache2
```

2. Implementar headers de seguridad en /etc/apache2/apache2.conf:

```
Header always set X-Content-Type-Options "nosniff"
```

```
Header always set X-Frame-Options "SAMEORIGIN"
```

```
Header always set X-XSS-Protection "1; mode=block"
```

```
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
```

3. Limitar tasa de conexiones:

```
<IfModule mod_ratelimit.c>
```

```
LimitRequestFields 50
```

```
LimitRequestFieldSize 8190
```

```
LimitRequestLine 4094
```

```
</IfModule>
```

5.3. Firewall y Acceso de Red (CORTO PLAZO)

Si el servidor no necesita estar expuesto públicamente, usar iptables:

```
$ sudo iptables -A INPUT -p tcp --dport 80 -s 192.168.5.0/24 -j ACCEPT
```

```
$ sudo iptables -A INPUT -p tcp --dport 80 -j DROP
```

2. Usar un WAF (Web Application Firewall):

- ModSecurity para Apache

- Cloudflare (si es accesible remotamente)

5.4. Monitoreo Continuo (PERMANENTE)

1. Suscribirse a alertas de seguridad de Apache:

<https://httpd.apache.org/security/>

2. Usar herramientas de monitoreo:

- Fail2ban para detectar intentos de ataque
- auditd para logging de cambios

3. Auditorías regulares:

\$ nmap -sV --script=vuln <IP> # Cada 2 semanas

6. Conclusiones

El sistema Debian analizado tiene una superficie de ataque reducida (solo puerto 80 abierto), pero la versión de Apache httpd instalada (2.4.65) contiene al menos 3 vulnerabilidades críticas de severidad alta que pueden permitir:

X Ejecución remota de código (CVE-2025-58098)

X Denegación de servicio (CVE-2025-59775)

X Inyección de contenido (CVE-2025-55753)

ACCIONES RECOMENDADAS POR PRIORIDAD:

[1] CRÍTICA: Actualizar Apache httpd a 2.4.66+ en 24-48 horas

[2] ALTA: Implementar headers de seguridad inmediatamente

[3] MEDIA: Aplicar restricciones de firewall

[4] BAJA: Monitoreo continuo y auditorías periódicas

El equipo de seguridad debe dar seguimiento a estas recomendaciones y verificar la implementación de parches dentro del próximo ciclo de actualización.