

# Inseguridades

## ■ MySQL

MySQL es un servidor de bases de datos multi-usuario y multi-hebra. Se han informado de varios problemas de seguridad que afectan al paquete mysql-server. Oleksandr Byelkin descubrió que el "ALTER TABLE ... RENAME" comprobaba los derechos CREATE/INSERT de la antigua tabla, en vez de los de la nueva. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-0835 a este problema. Lukas Wojtow descubrió una sobrescritura de búfer en la función

mysql\_real\_connect. Para poder explotar este problema, un atacante tendría que forzar el uso de un servidor DNS malicioso (CAN-2004-0836). Dean Ellis descubrió que múltiples hebras que ALTERasen el mismo (o diferentes) tablas MERGE para cambiar la UNION, podrían provocar un cuelgue o parada del servidor (CAN-2004-0837). Sergei Golubchik descubrió que si a un usuario se le otorgaban privilegios para un base de datos cuyo nombre contuviera un guión bajo ("\_"), también adquiriría la habilidad de ceder privilegios a otras bases de datos con nombres similares (CAN-2004-0957). También se han des-

cubierto diversos pequeños errores relacionados con el sistema de bases de datos MySQL, algunos de los cuales plantean potenciales agujeros de seguridad. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado los nombres (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) CAN-2004-0381, CAN-2004-0388, CAN-2004-0457 a estos problemas de seguridad de MySQL. 6 ■

Referencia Gentoo: GLSA 200410-22/MySQL

Referencia Mandrake: MDKSA-2004:119  
Referencia Red Hat: RHSA-2004:569-1

## ■ IPTables

Fahem Mitha informa de que la instrucción iptables, una herramienta de administración para el filtrado de paquetes IPv4 y NAT, no siempre cargaba los módulos requeridos por sí mismo, tal y como debería hacer. Esto podría conllevar a que las reglas de un cortafuegos no se cargasen en el arranque del sistema. Esto provoca un fallo en la conexión con reglas suministradas al menos por lokkit. Se recomienda a los usuarios que actualicen su versión de iptables. ■

Referencia Debian: DSA-580-1 iptables  
Referencia Mandrake: MDKSA-2004:125  
Referencia Suse: SUSE-SA:2004:037

## ■ Apache

El servidor HTTP Apache es uno de los más populares servidores web en Internet. mod\_include es un módulo Apache que maneja inclusiones por el lado del servidor (SSI). Existe un posible desbordamiento de búfer en la función get\_tag() de mod\_include.c. Si las inclusiones por el lado del servidor están habilitadas, un atacante local podría ser capaz de correr código arbitrario con los derechos de un proceso hijo httpd haciendo uso de un documento especialmente manipulado con SSI malformado. También se ha descubierto un desbordamiento de búfer basado en pila en mod\_proxy. mod\_ssl has sido actualizado de la versión mod\_ssl2.8.19-1.3.31 a la versión mod\_ssl2.8.21-1.3.32, lo que corrige un fallo que permitía a un cliente usar un cifrado que el servidor no considera lo suficientemente seguro. También existe un nuevo paquete PHP (php-4.3.9) para

## Políticas de seguridad de la Distribuciones Mayoritarias

Distribuidor	Fuente Seguridad	Comentario
Debian	Info: <a href="http://www.debian.org/security/">http://www.debian.org/security/</a> Lista: <a href="http://www.debian.org/debian-security-announce/">http://www.debian.org/debian-security-announce/</a> Referencia: DSA-...1)	Los avisos de seguridad actuales se incluyen en la página de inicio. Los avisos se proveen como páginas HTML con enlaces a los parches. Los avisos también incluyen una referencia a la lista de correo.
Gentoo	Info: <a href="http://www.gentoo.org/security/en/index.xml">http://www.gentoo.org/security/en/index.xml</a> Foro: <a href="http://forums.gentoo.org/">http://forums.gentoo.org/</a> Lista: <a href="http://www.gentoo.org/main/en/lists.xml">http://www.gentoo.org/main/en/lists.xml</a> Referencia: GLSA-...1)	Los avisos de seguridad actuales para la lista Gentoo en el sitio web de seguridad de Gentoo enlazan desde la página principal. Los avisos se presentan en HTML con códigos para fusionar las versiones corregidas.
Mandrake	Info: <a href="http://www.mandrakesecure.net">http://www.mandrakesecure.net</a> Lista: <a href="http://www.mandrakesecure.net/en/mlist.php">http://www.mandrakesecure.net/en/mlist.php</a> Referencia: MDKSA-...1)	Mandrakesoft posee su propios sitio web que versa sobre temas relacionadas con la seguridad. Entre otras cosas, incluye de avisos seguridad y referencias a las listas de correo. Los avisos son páginas HTML, pero no contienen enlaces a los parches.
Red Hat	Info: <a href="http://www.redhat.com/errata/">http://www.redhat.com/errata/</a> Lista: <a href="http://www.redhat.com/mailman/listinfo/">http://www.redhat.com/mailman/listinfo/</a> Referencia: RHSA-...1)	Red Hat archiva los fallos de seguridad bajo lo que denominan <i>erratas</i> . A continuación los problemas para cada versión de Red Hat se agrupan. Los avisos de seguridad se proveen como una página HTML con enlaces a los parches.
Slackware	Info: <a href="http://www.slackware.com/security">http://www.slackware.com/security</a> Lista: <a href="http://www.slackware.com/lists/(slackware-security)">http://www.slackware.com/lists/(slackware-security)</a> Referencia: [slackware-security]...1)	La página de inicio contiene enlaces al archivo de seguridad de la lista de correo. No existe información adicional sobre seguridad en Slackware.
Suse	Info: <a href="http://www.suse.de/en/private/support/security/index.html">http://www.suse.de/en/private/support/security/index.html</a> Parches: <a href="http://www.suse.de/en/private/download/updates">http://www.suse.de/en/private/download/updates</a> Lista: <a href="http://www.suse.de/en/private/download/updates">suse-security-announce</a> Referencia: SUSE-SA-...1)	Ya no existe un enlace a la página de seguridad tras un remodelado en el sitio web de SuSE. Existe información en la lista de correos y los avisos. Los parches de seguridad para versiones individuales de SuSE Linux se muestran de color rojo en el sitio de actualizaciones generales. Contiene una corta descripción de la vulnerabilidad que el parche soluciona.

1) Todos los distribuidores muestran correos de seguridad en el campo Subject.

todas estas plataformas. Se pueden consultar más detalles sobre estos problemas en la base de datos del proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>). Véase CAN-2004-0492 y CAN-2004-0885. ■

*Referencia Gentoo: GLSA 200411-03/apache*

*Referencia Mandrake: MDKSA-2004:122*

*Referencia Slackware: SSA:2004-305-01*

## ■ ImageMagick

ImageMagick(TM) es una herramienta de manipulación de imágenes para el sistema X Windows. Se ha descubierto un fallo de desbordamiento de pila en el manejador de imágenes de ImageMagick. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-0827 a este problema. ■

*Referencia Gentoo: GLSA 200411-11/imagemagick*

*Referencia Red Hat: RHSA-2004:466-12*

## ■ Libtiff

libtiff es utilizado por visualizadores de imágenes y navegadores web para mostrar imágenes "TIFF". Chris Evans descubrió varios fallos de seguridad durante una auditoría de la librería de manipulación de imágenes libtiff, algunos relacionados con desbordamientos de búfers, otros relacionados con desbordamientos de enteros y similares. Este problema se sigue en CVE ID CAN-2004-0803. Matthias Claasen encontró una división por cero en libtiff. Este problema tiene su seguimiento en CVE ID CAN-2004-0804. Otras auditorías llevadas a cabo por Dmitry Levin expuso varios otros desbordamientos de enteros, el seguimiento de los cuales se lleva a cabo en CVE ID CAN-2004-0886. iDEFENSE Security descubrió un desbordamiento de búfer en el manejo que hace el paquete libtiff de OJPEG (old JPEG) bajo SUSE. Esto se arregló deshabilitando el soporte para old JPEG y se realiza un seguimiento del problema en CVE ID CAN-2004-0929. ■

*Referencia Mandrake: MDKSA-2004:109*

*Referencia Red Hat: RHSA-2004:577-16*

*Referencia Slackware: SSA:2004-305-02*

*Referencia Suse: SUSE-SA:2004:038*

## ■ Squid

Squid es un cache de proxy web con muchas prestaciones. iDEFENSE Security informa de un fallo en el módulo de SNMP de squid. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-0918 a este problema. ■

*Referencia Debian: DSA-576-1 squid*

*Referencia Gentoo: GLSA 200410-15/squid*

*Referencia Mandrake: MDKSA-2004:112*

*Referencia Red Hat: RHSA-2004:591-04*

## ■ Gaim

La aplicación gaim es un cliente de mensajería instantánea multi-protocolo. Se ha descubierto un desbordamiento de búfer en el manejador del protocolo MSN. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-0891 a este problema. ■

Los paquetes actualizados gaim también arreglan errores en el interfaz de usuarios múltiples, de protocolos y de manejo de errores, incluyendo un problema con la codificación de comunicación ICQ. ■

*Referencia Gentoo: GLSA 200410-23/gaim*

*Referencia Red Hat: RHSA-2004:604-05*

*Referencia Slackware: SSA:2004-239-01*

## ■ CUPS

El Common UNIX Printing System (Sistema de Impresión Común UNIX o CUPS) es una cola de impresión. Durante una auditoría de código fuente, Chris Evans descubrió una serie de errores de desbordamiento de entero que afectan a xpdf. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-0888 a este problema de seguridad. Cuando se configura para imprimir en una impresora compartida a través de Samba CUPS se autentifica con esa impresora compartida utilizando un nombre y una contraseña. Por defecto, el nombre de usuario y la contraseña utilizadas por CUPS para

conectar con la compartición Samba se escribe en el fichero de registro de errores. Un usuario local que tenga permisos de lectura de este fichero de registro de errores podría cosechar estos nombres de usuario y contraseñas. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-0923 a este problema. ■

*Referencia Debian: DSA-581-1 xpdf*

*Referencia Mandrake: MDKSA-2004:116*

*Referencia Red Hat: RHSA-2004:543-15*

*Referencia Suse: SUSE-SA:2004:039*

## ■ webmin

webmin es un kit de herramientas de administración basadas en web. Ludwig Nussel ha descubierto un problema cuando un directorio temporal se utiliza pero no se comprueba el dueño previo. ■

*Referencia Debian: DSA-544-1*

*Referencia Mandrake: MDKSA-2004:101*

## ■ KDE

KDE es un entorno de escritorio para sistemas Unix y Linux.

La integridad de los enlaces simbólicos utilizados por KDE no se pueden asegurar y, como resultado, pueden ser abusados por atacantes locales para crear o truncar ficheros arbitrarios o evitar que aplicaciones KDE funcionen correctamente (CAN-2004-0689).

Konqueror permite a sitios web cargar páginas web en un marco de cualquier otra página basada en web que el usuario pudiera tener abierto. Konqueror también permite establecer cookies para ciertos dominios nacionales de primer nivel. Todos aquellos dominios nacionales de primer nivel que utilizan más de dos caracteres en la parte secundaria del nombre de dominio se encuentran afectados, al igual que aquellos que utilizan una parte secundario que no sea uno de los siguientes: com, net, mil, org, gove, edu o int (CAN-2004-0746 y CAN-2004-0721) ■

*Referencia Debian: DSA-539-1 kdelibs*

*Referencia Mandrake: MDKSA-2004:086*

*Referencia Slackware: DSA-539-1 kdelibs - directorio vulnerabilidades temporal*