

# INSEGURIDADES

## ■ Quagga

Quagga, que administra el protocolo de enrutado basado en TCP/IP, utiliza un método multiservidor y multi-hilo para resolver la complejidad actual de Internet.

Se encontró un fallo en la manera en la que Quagga interpreta paquetes RIP REQUEST. RIPd en Quagga responderá a paquetes RIP REQUEST para versiones RIP que han sido deshabilitadas o que tienen autenticación habilitada, permiti-

tiendo a un atacante remoto adquirir información sobre la red local. (CVE-2006-2223)

Se encontró un fallo de inyección de ruta en la manera en la que Quagga interpreta paquetes RIPv1 RESPONSE cuando está habilitada la autenticación RIPv2. Un atacante remoto que conoce este fallo puede inyectar información de ruta arbitraria en las tablas routing RIPd. Este problema no afecta a las configuraciones Quagga donde solamente está especificada RIPv2. (CVE-2006-2224)

Se encontró un fallo de denegación de servicio en la interfaz telnet de Quagga. Si un atacante puede conectarse a la interfaz telnet de Quagga es posible que haga que éste consuma grandes cantidades de recursos de la CPU a través de un comando sh malformado. (CVE-2006-2276) ■

Referencia Debian: DSA-1059-1

Referencia Gentoo: GLSA 200605-15

Referencia Red Hat: RHSA-2006:0525-5

## ■ Quake3

Quake3 es un shooter de primera persona multijugador.

landser descubrió una vulnerabilidad en el comando remapshader. Debido a un error en la manipulación del límite en remapshader, existe la posibilidad de un desbordamiento de búfer.

Un atacante podría establecer un servidor de juego malicioso y tentar a los usuarios a conectarse, ejecutando código arbitrario potencialmente con los derechos de un usuario del juego. ID CVE-2006-2007 ■

Referencia Gentoo: GLSA 200605-15

## ■ Cron

Vixie cron es el demonio CRON por defecto en todas las distribuciones basadas en Linux SUSE.

El código en do\_command.c en Vixie Cron no comprueba el código de vuelta de una llamada setuid, lo cual podría permitir que los usuarios locales consigan privilegios root si falla setuid en casos como fallos PAM o límites de recursos. Este problema es conocido por afectar solamente a distribuciones con kernels 2.6 de Linux. Es seguido por Mitre CVE ID CVE-2006-2607. ■

Referencia Suse: SUSE-SA:2006:027

## ■ Nagios

Nagios es una herramienta de monitorización de red de código abierto.

### POLITICAS DE SEGURIDAD DE LAS 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 relacionados con la seguridad. Entre otras cosas, incluye 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: suse-security-announce 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 soluciona el parche.

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

Existe un desbordamiento de número entero en la manipulación de cabeceras HTTP por CGIs. Esta condición podría llevar a la ejecución de código arbitrario por atacantes remotos en nombre de Nagios. Se ha asignado a este problema el nombre CVE-2006-2162. **n**

*Referencia Debian: DSA-1072-1*

*Referencia Suse: SUSE-SR:2006:011*

## ■ OpenOffice

OpenOffice es una suite de productividad ofimática que incluye aplicaciones de escritorio como un procesador de textos, hoja de cálculo, administrador de presentaciones, editor de fórmulas y un programa de diseño.

Un especialista en seguridad de Sun ha informado de un problema con la infraestructura de aplicaciones. Un atacante podría colocar macros en un documento que serían ejecutadas por OpenOffice.org cuando una víctima las abriese. (CVE-2006-2198).

Se encontró un error en la implementación de la máquina virtual de Java de OpenOffice.org. Un atacante podría escribir una applet Java cuidadosamente manipulado que podría salir de la "caja de arena" (zona de pruebas) y obtener acceso completo a recursos del sistema con los privilegios del usuario actual. (CVE-2006-2199).

Se encontró un error de desbordamiento de búfer en el procesador de ficheros de OpenOffice.org. Un atacante podría crear un fichero XML cuidadosamente manipulado que hiciera que OpenOffice.org escribiera datos a un lugar arbitrario en memoria cuando el fichero fuese abierto por la víctima. (CVE-2006-3117). **■**

*Referencia Debian: DSA-1104-2*

*Referencia Mandriva: MDKSA-2006:118*

*Referencia Red Hat: RHSA-2006:0573-10*

*Referencia Suse: SUSE-SA:2006:040*

## ■ wv2

wv2 es una librería filtro para ficheros de Microsoft Word que se utiliza en muchas suites ofimáticas.

Se encontró un error de comprobación de límite en wv2 que podría desencadenar un desbordamiento de entero. Un atacante podría ejecutar código arbitrario con los privilegios del usuario que ejecuta el programa que utiliza la librería con un documento de

Microsoft Word maliciosamente manipulado. **■**

*Referencia Debian: DSA-1100-1 wv2*

*Referencia Gentoo: GLSA 200606-24*

*Referencia Mandriva: MDKSA-2006:109*

*Referencia Suse: SUSE-SR:2006:015*

## ■ aRts

aRts es un sistema de síntesis de audio utilizado por KDE modular y en tiempo real. artswrapper es una aplicación asistente que se utiliza para arrancar el demonio aRts.

artswrapper no comprueba correctamente si puede bajar los privilegios si *setuid()* falla, debido a que un usuario se excede de los límites de recursos asignados.

Atacantes locales podrían explotar esta vulnerabilidad para ejecutar código arbitrario con privilegios elevados. **■**

*Referencia Gentoo: GLSA 200606-22*

*Referencia Mandriva: MDKSA-2006:107*

*Referencia Slackware: SSA:2006-178-03*

*Referencia suse: SUSE-SR:2006:015*

## ■ Kdebase

Los paquetes de kdebase aportan las aplicaciones centrales de KDE, el K Desktop Environment. Estos paquetes centrales incluyen el Administrador de Pantallas de KDE (KDM).

Ludwig Nussel ha descubierto un fallo en KDM. Un usuario local malicioso de KDM podría utilizar un ataque de enlace blando para leer un fichero arbitrario que el usuario no tiene permiso de lectura. (CVE-2006-2449). **■**

*Referencia Gentoo: GLSA 200606-23*

*Referencia Mandriva: MDKSA-2006:105*

*Referencia Red Hat: RHSA-2006:0548-5*

*Referencia Slackware: SSA:2006-178-01*

*Referencia suse: SUSE-SR:2006:039*

## ■ Sendmail

Sendmail es un Agente de Transporte de Correo (MTA) utilizado para remitir correo electrónico.

Se ha descubierto en Snedmail un fallo en la manipulación de mensajes multi-parte MIME. Un atacante remoto podría crear un mensaje cuidadosamente manipulado que hiciera que Sendmail se colgase durante la entrega. (CVE-2006-1173). En muchos casos, Sendmail sólo está configurado para aceptar conexiones desde el host local. Por tanto, solamente aquellos administradores que hayan configurado

Sendmail para que escuche a máquinas remotas son susceptibles de sufrir esta vulnerabilidad. **■**

*Referencia Gentoo: GLSA 200606-19*

*Referencia Mandriva: MDKSA-2006:104*

*Referencia Red Hat: RHSA-2006:0515-14*

*Referencia Slackware: SSA:2006-166-01*

*Referencia suse: SUSE-SA:2006:032*

## ■ FreeType

FreeType es un motor de fuentes por software. Un subdesbordamiento en las versiones de FreeType anteriores a 2.2 permiten a un atacante provocar una denegación de servicio (cuelgue del sistema) con un fichero de fuentes con un número impar de valores azules, lo que provoca el subdesbordamiento cuando se decreta de 2 en 2 en un contexto que espera un número par de valores. (CVE-2006-0747).

Múltiples desbordamientos de enteros en versiones anteriores a 2.2 permiten a atacantes remotos provocar una denegación de servicio (cuelgue del sistema) y posible ejecución de código arbitrario a través de vectores de ataque relacionados con (1) *bdf/dflib.c*, (2) *sfnt/ttmap.c*, (3) *cff/cffgload* y (4) la función *read\_lwnf* y un fichero LFWN manipulado en *base/ftmac.c*. (CVE-2006-1861).

*Ftutil.c* en versiones de FreeType anteriores a 2.2 permite a atacantes remotos provocar una denegación de servicio (cuelgue del sistema) con un fichero de fuente manipulado que desencadena un desreferencia de nulo. (CVE-2006-2661). **■**

*Referencia Debian: DSA-1095-1*

*Referencia Mandriva: MDKSA-2006:099-1*

## ■ MySQL

MySQL es un servidor SQL multi-hilo y multi-usuario muy extendido.

Un atacante podría leer porciones de memoria utilizando un nombre de usuario seguido de un byte NULO o utilizando el comando *COM\_TABLE\_DUMP* (CVE-2006-1516, CVE-2006-1517).

Un atacante podría ejecutar código arbitrario provocando un desbordamiento de búfer con unos paquetes *COM\_TABLE\_DUMP* que estuvieran especialmente manipulados (CVE-2006-1518). **■**

*Referencia Gentoo: GLSA 200606-13*

*Referencia Mandriva: MDKSA-2006:111*

*Referencia suse: SUSE-SA:2006:036*