

# INSEGURIDADES

## Adobe Flash Player

Adobe ha anunciado tres problemas de seguridad en su Flash Player. Las versiones de Adobe Flash Player 9.0.45.0 y anteriores tienen un error de desbordamiento de entero que permitiría que atacantes remotos ejecutaran código arbitrario. (CVE-2007-3456)

Las versiones de Adobe Flash Player 8.0.34.0 y anteriores no validan apropiadamente las cabeceras HTTP. (CVE-2007-3457)

Las versiones de Adobe Flash Player 7 y 9, cuando se usan con versiones de Opera anteriores a la 9.20 o con Konqueror anteriores a 20070613, permite a atacantes remotos obtener información sen-

sible (tecleos en el navegador), que es filtrada al applet de Flash Player. (CVE-2007-2022) ■

Referencia SUSE: SUSE-SA:2007:45

Referencia Red Hat: RHSA-2007:0385-4

## Defectos de BIND

En las versiones de BIND 9.4.0, 9.4.1 y 9.5.0a1 hasta 9.5.0a5, las listas de control de acceso por defecto (ACLs) no se han establecido correctamente, de manera que cualquiera podría realizar consultas recursivas o bien consultar los contenidos de la caché. (CVE-2007-2925)

Se descubrió un fallo en el generador del número de secuencia. Las versiones de BIND 9 hasta la 9.5.0a5 usan un generador

de números al azar débil durante la creación de IDs de consulta de DNS cuando responde a consultas del codificador o cuando envía mensajes NOTIFY para esclavizar a los servidores de nombres, lo que hace que sea más fácil para atacantes remotos adivinar la siguiente consulta ID y llevar a cabo un envenenamiento de la caché DNS. (CVE-2007-2926) ■

Referencia Red Hat: RHSA-2007:0740-2

Referencia Mandriva: MDKSA-2007:149

Referencia Ubuntu: USN-491-1

## Vulnerabilidades de Firefox y IceWeasel

Recientemente han sido descubiertos algunos fallos en la manera en la que Firefox procesa algunos tipos de código JavaScript malformado. Una página web que contenía código JavaScript malicioso podría hacer que Firefox se colgara o que potencialmente ejecutara código arbitrario con los permisos del usuario ejecutando Firefox. (CVE\_2007-3734, CVE-2007-3735, CVE-2007-3237, CVE-2007-3738)

Se encontraron algunos fallos de inyección de contenido en la manera en la que Firefox maneja ciertos códigos JavaScript. Una página web con código JavaScript hostil podría inyectar contenido arbitrario a otras páginas web. (CVE-2007-3736, CVE-2007-3089)

Se encontró un error en la manera en la que Firefox cachea páginas web en el disco local. Una página web maliciosa puede hacer que se inyecte código HTML arbitrariamente en una sesión de navegación si el usuario vuelve a cargar un sitio guardado. (CVE-2007-3656) ■

Referencia Red Hat: RHSA-2007:0724-4

Referencia Debian: DSA-1338-1

Referencia Ubuntu: USN-490-1

## libcurl

Las versiones de libcurl desde la 7.14.0 hasta la 7.16.3, cuando compilan con el soporte GnuTLS, no comprueban la fecha de caducidad de SSL/TLS o las fechas de activación, lo que permite a los atacantes remotos evitar ciertas restricciones de acceso. (CVE-2007-3564) ■

Referencia Debian: DSA-1333-1

Referencia Ubuntu: USN-484-1

## 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 propio sitio web que versa sobre temas relacionados con la seguridad. Entre otras cosas, incluye avisos de 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*.

### IX.org

El servidor de fuentes xfs de X.Org X11 proporciona un mecanismo estándar para que un servidor X se comunique con un renderizador de fuentes. En Red Hat Enterprise 5 y Fedora Core 6, se encontró un fallo en el fichero temporal en la manera en la que el servidor de fuentes xfs de X.Org X11 ejecuta los scripts de arranque. Un usuario local podría modificar los permisos de un fichero de su elección, elevando posiblemente sus privilegios locales. (CVE-2007-3103) ■

Referencia Red Hat: RHSA-2007:0520-2

### ClamAV

Hay un fallo en el programa RAR VM (*unrarvm.c*) que forma parte del antivirus Clam (ClamAV) anterior a la versión 0.91. El fallo permite a atacantes remotos asistidos por el usuario causar una denegación de servicio a través de un archivo RAR manipulado, dando lugar a una desreferencia de un puntero NULL. (CVE-2007-3725) ■

Referencia Debian: DSA-1340-1

Referencia Mandriva: MDKSA-2007:150

### NVClock

NVClock es una pequeña utilidad que permite incrementar la velocidad del chip de la CPU en sus tarjetas de vídeo. Debido a un fallo en la función *set\_default\_speeds* en las funciones *backend/backend.c* anteriores a la versión 0.8b2, los usuarios locales tienen permitido sobreescibir ficheros arbitrarios a través de un ataque symlink en el fichero temporal */tmp/nvclock*. (CVE-2007-3531) ■

Referencia Gentoo: GLSA-200707-08/nvclock

### GIMP

La versión 2.2.15 de GIMP tiene un problema de desbordamiento de entero con la función *seek\_to\_and\_unpack\_pixeldata* del plugin *psd.c*. Este problema podría permitir a un atacante remoto ejecutar código arbitrario si manipula un fichero PSD que contiene una altura o anchura grande y un usuario lo abre. (CVE-2007-2949) ■

Referencia Debian: DSA-1335-1

Referencia Ubuntu: USN-480-1

### GSAMBAD

GSAMBAD es un front-end basado en Gtk+ para el servidor de impresión y el fichero Samba. Un problema con la función *populate\_conns* en *src/populate\_conns.c* de la versión 0.1.4 permite a usuarios locales sobreescibir ficheros arbitrarios mediante un ataque symlink al fichero temporal */tmp/gsambadtmp*. (CVE-2007-2838) ■

Referencia Debian: DSA-1327-1

### Festival

Se ha descubierto una vulnerabilidad en Festival, una utilidad de síntesis de voz para textos, que permite una escalada de privilegios locales. La configuración Gentoo de Festival por defecto tiene el demonio configurado para ejecutarse con privilegios root y para escuchar en localhost, todo sin necesidad de contraseña. Un atacante local podría obtener privilegios de root conectándose al demonio y ejecutando luego comandos arbitrarios. ■

Referencia Gentoo: LSA-200707-10/festival

