

INSEGURIDADES

vim

El cajón de arena de vim permite peligrosas funciones, como *writefile*, *feedkeys* y *system*, que podrían permitir que atacantes asistidos por usuarios ejecutaran comandos de la shell y escribieran ficheros vía modelos. (CVE-2007-2438) ■

Referencia Mandriva: MDKSA-2007:101

Referencia Red Hat: RHSA-2007:0346-3

Referencia SUSE: SUSE-SR:2007:012

Referencia Ubuntu: USN-463-1

FreeType

FreeType no verificaba correctamente el número de puntos en una fuente TrueType. Si un usuario fuera engañado para que usara una fuente especialmente manipu-

lada, un atacante podría ejecutar código arbitrario con privilegios de ese usuario. (CVE-2007-2754) ■

Referencia Gentoo: GLSA 200705-22

Referencia Ubuntu: USN-466-1

PHP

Se ha descubierto un fallo en el manipulador de comandos ftp de PHP. Los comandos no se filtra correctamente los caracteres de control, y un atacante podría dar comandos ftp arbitrarios usando argumentos especialmente manipulados. Un desbordamiento de búfer en el manipulador de peticiones SOAP en PHP podría permitir que atacantes remotos enviaran peticiones SOAP especialmente manipuladas y ejecu-

tan código arbitrario con los privilegios de un servidor web. Un desbordamiento de búfer en la fabricación del filtro de usuario en PHP podría permitir que un atacante local creara un script especialmente manipulado y ejecutara código arbitrario con los privilegios de un servidor web. El instalador PEAR no valida las rutas de instalación, de modo que si un usuario instaló un paquete PEAR malicioso, un atacante podría sobrescribir ficheros arbitrarios. (CVE-2007-2509, CVE-2007-2510, CVE-2007-2511, CVE-2007-2519) ■

Referencia Debian: DSA-1280-1

Referencia Mandrake: MDKSA-2007:102, MDKSA-2007:103

Referencia Red Hat: RHSA-2007:0348,

RHSA-2007:0349, RHSA-2007:0355

Referencia Ubuntu: USN-462-1

Firefox, SeaMonkey y Thunderbird

Se ha descubierto una vulnerabilidad en la que el protocolo APOP permite a los atacantes remotos adivinar los tres primeros caracteres de una contraseña a través de ataques hombre-en-medio (MITM) que usan mensajes manipulados y colisiones MD5 e IDs.

El problema a nivel de diseño afecta potencialmente a todos los productos APOP, incluyendo Thunderbird, Evolution, Mutt, fetchmail y SeaMonkey.

Múltiples vulnerabilidades en el motor de formato de Mozilla Firefox, Thunderbird y SeaMonkey permiten a atacantes remotos causar una denegación de servicio a través de vectores relacionados con punteros colgantes, corrupciones de pila, con o sin signo y otros problemas. Numerosas vulnerabilidades en el motor JavaScript permiten a los atacantes remotos causar una denegación de servicio y posiblemente ejecutar código arbitrario mediante vectores que desencadenan corrupción de memoria. (CVE-2007-1558, CVE-2007-2867, CVE-2007-2868) ■

Referencia Mandriva: MDKSA-2007:105

Referencia Red Hat: RHSA-2007:0353

Referencia Ubuntu: USN-469-1

Samba

Samba no abandonó completamente los privilegios root mientras traducía los SIDs.

POLITICAS DE SEGURIDAD DE LAS DISTRIBUCIONES MAYORITARIAS

Distribuidor	Fuente Seguridad	Comentario
Debian	Info: http://www.debian.org/security/ Lista: http://www.debian.org/debian-security-announce/ 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: http://www.gentoo.org/security/en/index.xml Foro: http://forums.gentoo.org/ Lista: http://www.gentoo.org/main/en/lists.xml 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: http://www.mandrakesecure.net Lista: http://www.mandrakesecure.net/en/mlist.php 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: http://www.redhat.com/errata/ Lista: http://www.redhat.com/mailman/listinfo/ 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: http://www.slackware.com/security Lista: http://www.slackware.com/lists/(slackware-security) 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: http://www.suse.de/en/private/support/security/index.html Parches: http://www.suse.de/en/private/download/updates 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*.

Un usuario remoto autenticado podría llevar a cabo operaciones SMB en un corto espacio de tiempo y obtener privilegios root.

Samba contiene algunos fallos cuando analiza parámetros RPC codificados con NDR. Falla al desinfectar adecuadamente la entrada al procedimiento remoto vía Microsoft Remote Procedure Calls. (CVE-2007-2444, CVE-2007-2446, CVE-2007-2447) ■

- Referencia Debian: DSA-1291
- Referencia Gentoo: GLSA-200705-15
- Referencia Mandrake: MDKSA-2007:104
- Referencia Slackware: SSA:2007-134-01
- Referencia SUSE: SUSE-SA:2007:031
- Referencia Ubuntu: USN-460-1

SquirrelMail

Múltiples vulnerabilidades del scripting multitisio (XSS) en el filtro HTML de SquirrelMail 1.4.0 a 1.4.9a permiten a atacantes remotos inyectar scripts web arbitrarios o HTML mediante los datos: URI en un adjunto de correo HTML, o varios juegos de caracteres no-ASCII que no se filtran adecuadamente cuando se ven con Microsoft Internet Explorer. (CVE-2007-1262) ■

- Referencia Debian: DSA-1290

- Referencia Mandriva: MDKSA-2007:106
- Referencia Red Hat: RHSA-2007:0358

file

Un desbordamiento de entero en el programa file 4.20, cuando se ejecuta en sistemas de 32-bits, podría permitir que atacantes asistidos por usuarios ejecutaran código arbitrario a través de un fichero grande, desencadenando un desbordamiento que evitaría una instrucción assert(). ■

- Referencia Gentoo: GLSA-200705-25
- Referencia Mandriva: MDKSA-2007:114
- Referencia Red Hat: RHSA-2007:0391-3

GIMP

Un desbordamiento de búfer basado en pila en la función set_color_table en sunras.c en el plugin SUNRAS en GIMP 2.2.14 permite a atacantes remotos asistidos por un usuario ejecutar código arbitrario mediante un fichero RAS manipulado. (CVE-2007-2356) ■

- Referencia Gentoo: GLSA-200705-08
- Referencia Mandriva: MDKSA-2007:108
- Referencia Red Hat: RHSA-2007:0343
- Referencia SUSE: SUSE-SR:2007:011
- Referencia Ubuntu: USN-467-1

PPTPD

Se descubrió una vulnerabilidad en PPTPD, un demonio para el protocolo de tunelado punto-a-punto para Linux. El fallo permitiría a atacantes remotos enviar un paquete especialmente manipulado e interrumpir túneles PPTPD establecidos, llevando a una denegación de servicio. (CVE-2007-0244) ■

- Referencia Debian: DSA-1288-1 pptpd
- Referencia Gentoo: GLSA-200705-18
- Referencia SUSE: SUSE-SR:2007:010

PSec

Se descubrió un fallo en el servidor de intercambio de claves IPsec "racoon". Atacantes remotos podrían enviar un paquete especialmente manipulado e interrumpir los túneles IPsec establecidos, llevando a una denegación de servicio. (CVE-2007-1841) ■

- Referencia Gentoo: GLSA-200705-09
- Referencia Mandriva: MDKSA-2007:084
- Referencia Red Hat: RHSA-2007:0342
- Referencia SUSE: SUSE-SR:2007:008
- Referencia Ubuntu: USN-450-1

