

INSEGURIDADES

KDE

KDE es uno de los más populares programas de administración de escritorios para Linux, y está incluido en un gran número de distribuciones.

Un fallo en las versiones 3.3.0 hasta 3.5.7 puede permitir que atacantes remotos se salten los requerimientos de contraseñas y se registren en cuentas arbitrarias. Para que los atacantes exploten este fallo deben estar deshabilitadas las opciones de "shutdown with password" y las de autologin. (CVE-2007-4569)

También, una página web hostil podría engañar a la barra de direcciones de Konqueror mostrando una página

web distinta a la que se muestra realmente. (CVE_2007-3820, CVE_2007-4224) ■

Referencia Debian: DSA-1376-1

Referencia Red Hat: RHSA-2007:0905-1

Referencia Ubuntu: USN-517-1

jffnms

jffnms (Just Fun Network Management System) es un programa basado en web que permite monitorizar cualquier dispositivo compatible con los estándares SNMP. Han aparecido tres problemas en jffnms.

Un problema es que tolera scripting multisitio XSS, lo que permite a atacantes remotos inyectar un script web

arbitrario o código HTML a través del parámetro de usuario. (CVE-2007-3189)

Existen múltiples aberturas para la inyección de SQL en auth.php cuando se encuentra deshabilitada la opción `magic_quotes_gpc`. Un atacante remoto podría ejecutar comandos SQL arbitrarios. (CVE-2007-3190)

Un problema en el script admin/setup.php permite a atacantes remotos leer y modificar las opciones de configuración. (CVE-2007-3192) ■

Referencia Debian: DSA-1374-1

xorg-server

xorg-server es una referencia para el sistema X Window y un componente esencial de la mayoría de las GUIs de las distribuciones Linux. Cualquier problema con xorg-server afecta a casi todas las máquinas actuales con escritorio Linux.

Ha aparecido un problema de desbordamiento de búfer en la función `compNewPixmap` de `compalloc.c` en las extensiones Composite de xorg-server. Un usuario local podría usar este fallo para ejecutar código arbitrario copiando los datos de un mapa de píxeles de gran profundidad a otro de menor profundidad. (CVE-2007-4730) ■

Referencia Debian: DSA-1372-1

Referencia Ubuntu: USN-514-1

Fetchmail

Fetchmail es un popular programa de correo IMAP, POP3 y APOP. Fetchmail recupera correo de un servidor remoto a través de un protocolo preferente del servidor remoto y luego remite el mensaje a la máquina local en protocolo SMTP. Esto permite a los paquetes que requieren SMTP poder funcionar en los sitios en los que de otra manera serían inservibles.

En versiones de Fetchmail anteriores a la 6.3.9 es posible para un servidor de correo hostil hacer que Fetchmail se cuelgue negándose a aceptar determinados mensajes de aviso SNMP. (CVE-2007-4565) ■

Referencia Debian: DSA-1377-2

Referencia Ubuntu: USN-520-1

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*.

PhpWiki

PhpWiki es un sistema de documentación escrito en lenguaje de programación PHP. Han surgido distintos problemas con él.

PhpWiki no lleva a cabo un trabajo correcto de validación de nombre de fichero, lo que puede permitir descargas de ficheros ilimitadas. (CVE-2007-2024, CVE-2007-2025)

Si el fichero de configuración no tiene un `PASSWORD_LENGTH_MINIMUM` sin cero, entonces, dependiendo de la versión de LDAP que se ejecute en el sistema, un atacante podría ser capaz de evitar la autenticación. (CVE-2007-3193)

Referencia Debian: DSA-1371-1

Referencia Gentoo:GLSA 200709-10

Xen

Xen es una utilidad que permite que a un solo ordenador se le configuren múltiples máquinas virtuales. Un problema en Xen consiente que uno de los sistemas operativos huésped ejecute programas bajo el maestro, albergando un sistema operativo mediante

un fichero `grub.com` especialmente manipulado. (CVE-2007-4993)

Referencia Debian: DSA-1384-1

Referencia Ubuntu: USN-527-1

xfs

X Font Server, xfs, es un programa servidor central para la generación de imágenes de fuentes. En los últimos años ha dejado de ser el favorito, siendo a menudo reemplazado por programas de renderización de fuentes basados en el cliente, como Xft2 o Cairo.

Problemas de desbordamiento de entero dentro de la función `build_range` podrían permitir que un atacante ejecutara código arbitrario. También, una petición QueryXExtends especialmente manipulada podría desencadenar un desbordamiento de búfer basado en pila. (CVE-2007-4568)

Referencia Debian: DSA-1385-1

OpenOffice

OpenOffice es una popular suite ofimática para sistemas Linux.

Se ha descubierto un problema de desbordamiento de entero en el analizador de imagen TIFF. Un atacante podría conseguir que OpenOffice ejecutara código arbitrario creando un fichero de imagen TIFF especialmente manipulado. (CVE-2007-2834)

Referencia Debian: DSA-1376

Referencia

SUSE:

SUSE-SA:2007:052

Referencia Ubuntu: USN-524-1

KVirc

KVirc es un cliente IRC libre y portable basado en Qt. Un error en la función `paesrlrcUrl()` no valida correctamente la URL cuando crea comandos para el sistema de script interno de KVirc. Si un usuario abre un URL `irc://` especialmente manipulado, el sitio remoto podría ejecutar código arbitrario en el sistema del usuario. KVirc debe ser el manipulador predeterminado `irc://` para que este exploit funcione. (CVE-2007-2951)

Referencia Gentoo:GLSA 200709-02

