

INSEGURIDADES

kdelibs

El paquete kdelibs proporciona librerías para el Entorno de Escritorio K (K Desktop Environment, KDE).

La librería khtml de KDE usa Qt de manera que los parámetros no validados podrían pasarse a Qt, dando lugar a un desbordamiento. Un atacante podría, por ejemplo, crear una página web maliciosa que, cuando fuera visitada por una víctima en el navegador Konqueror, haría que Konqueror se colgara o posiblemente ejecutara código arbitrario con los privilegios de la víctima (CVE-2006-4811). ■

Referencia Mandriva: MDKSA-2006:186
Referencia Red Hat: RHSA-2006:0720-5

Mono

Mono es una infraestructura .NET de Código Abierto. Sebastián Kraemer del equipo de seguridad de Suse encontró que las clases *System.CodeDom.Compiler* en mono usaban ficheros temporales de manera insegura, lo que podría permitir que el ataque de un enlace simbólico sobrescribiera ficheros arbitrarios con los privilegios de un usuario que corriera un programa que fuera usado por las mencionadas clases (CVE-2006-5072). ■

Referencia Mandriva: MDKSA-2006:188
Referencia Ubuntu: USN-357-1

OpenSSL

OpenSSL es un sistema de protocolo para seguridad en red. Dr. S. N. Henson, del

equipo de desarrollo de OpenSSL y de Open Network Security, ha desarrollado recientemente una suite de comprobación ASN1 para NISCC (www.niscc.gov.uk). Cuando la suite de comprobación fue ejecutada contra OpenSSL se descubrieron dos vulnerabilidades de denegación de servicio.

Durante el análisis de ciertas estructuras ASN1 no válidas, se manejó mal un error de condición. Esto puede dar lugar a un bucle infinito que consume la memoria del sistema (CVE-2006-2937).

Determinados tipos de claves públicas pueden tomarse un tiempo desproporcionado para ejecutar el proceso. Esto podría ser usado por un atacante durante un ataque de denegación de servicio. (CVE-2006-2940)

Tavis Ormandy y Will Drewry del Equipo de Seguridad de Google descubrieron un desbordamiento de búfer en la función de utilidad *SSL_get_shared_ciphers utility function*, usada por aplicaciones como *exim* y *mysql*. Un atacante podría enviar una lista de claves que podrían invadir un búfer. (CVE-2006-3738)

Ormandy y Drewry también descubrieron un posible DoS en el código de cliente *sslv2*. Si una aplicación cliente usa OpenSSL para efectuar una conexión *SSLv2* a un servidor malicioso, este servidor podría hacer que el cliente se colgara (CVE-2006-4343). ■

Referencia Debian: DSA-1195-1 Referencia Ubuntu: USN-353-2

Asterisk

Asterisk es una implementación de código abierto de una centralita telefónica digital (PBX).

Asterisk contiene desbordamientos de búfers en *channels/chan_mgcp.c* del driver MGCP y en *channels/chan_skinny.c* del driver del canal Skinny para teléfonos SCCP Cisco. También maneja peligrosamente variables controladas por clientes para determinar nombres de ficheros en la función *Record()*. Finalmente, el driver del canal SIP en *channels/chan_sip.c* puede usar más recursos de los necesarios bajo circunstancias no específicas.

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 atacante remoto podría ejecutar código arbitrario enviando una respuesta de punto-final de revisión manipulada (AUPEP), enviando un paquete Skinny overlay extenso incluso antes de la implementación o haciendo uso de especificadores de cadenas de formato a través de las variables controladas de cliente. También podría causar una denegación de servicio mediante el consumo de recursos a través del driver del canal SIP. ■

Referencia Gentoo: GLSA 200610-15

PHP

PHP es un lenguaje de scripting de uso general ampliamente usado, hecho a medida especialmente para desarrollo web.

El proyecto Hardened-PHP descubrió desbordamientos de búfers en rutinas internas `htmlentities/htmlspecialchars`. El propósito de estas funciones es recibir la entrada del usuario. El desbordamiento sólo se produce cuando se usa UTF-8 (CVE-2006-5465). ■

Referencia Gentoo: GLSA 200610-14
 Referencia Mandriva: MDKSA-2006:185
 Referencia Slackware: SSA:2006-230-02
 Referencia Suse: SUSE-SA:2006:059
 Referencia Ubuntu: USN-362-1

QT

Qt es un juego de herramientas de software que simplifica la tarea de escribir y de mantener aplicaciones GUI (Graphical User Interface) para el Sistema X Windows.

Se encontró un desbordamiento de número en la manera en la que Qt manipula ciertas imágenes de mapas de pixels. Si una aplicación vinculada a Qt crea una imagen pixmap, podría llevar a una denegación de servicio o posiblemente permitir la ejecución de código arbitrario (CVE-2006-4811). ■

Referencia Mandriva: MDKSA-2006:187
 Referencia Red Hat: RHSA-2006:0725-3
 Referencia Slackware: SSA:2006-298-01
 Referencia Suse: SUSE-SA:2006:063
 Referencia Ubuntu: USN-368-1

ClamAV

ClamAV es un antivirus de Código Abierto. Un desbordamiento de número en versiones anteriores de ClamAV podría permitir que un atacante remoto causara una denegación de servicio (scanning service crash) y ejecutara código arbitrario a través de un fichero Portable Executable (PE) (CVE-2006-4182).

Otra vulnerabilidad podría permitir que un atacante remoto causara un DoS a través de un fichero HTML comprimido manipulado haciendo que ClamAV leyera un lugar de memoria no válido (CVE-2006-5295). ■

Referencia Debian: DSA-1196-1
 Referencia Gentoo: GLSA 200610-10
 Referencia Mandriva: MDKSA-2006:184
 Referencia Suse: SUSE-SA:2006:060

Screen

Screen es un administrador de ventana de pantalla completa que multiplexa un terminal físico entre algunos procesos, típicamente shells interactivas.

Stoney y Rich Felker descubrieron un error de programación en el código de manipulación de cadenas UTF8 de Screen llevando posiblemente a una denegación de servicio. Si una cadena manipulada se presenta dentro de una sesión de Screen, éste podría colgarse o posiblemente ejecutar código arbitrario (CVE-2006-4573). ■

Referencia Debian: DSA-1202-1
 Referencia Gentoo: GLSA 200611-01
 Referencia Mandriva: MDKSA-2006:191
 Referencia Slackware: SSA:2006-307-02
 Referencia Ubuntu: USN-370-1

