

INSEGURIDADES

■ KRB5

Kerberos es un sistema de autenticación en red que utiliza un tercero de confianza (un KDC) para autenticar clientes y servidores entre sí.

El paquete krb5-workstation incluye un cliente telnet compatible con Kerberos. Se descubrieron dos desbordamientos de búfer en la manera en que el cliente telnet maneja mensajes del servidor. Un atacante podría ser capaz de ejecutar código arbitrario en la máquina del cliente si se consigue engañar a un usuario para que se conecte a un servidor telnet malicioso.

El proyecto de Vulnerabilidades y Exposiciones Comunes (Common

Vulnerabilities and Exposures o CVE – <http://cve.mitre.org>) ha asignado los nombres CAN-2005-0468 y CAN-2004-0469 a este problema. ■

-Referencia Debian: DSA-703-1 krb5

-Referencia Gentoo: GLSA 200504-04 /telnet

-Referencia Mandriva:

MDKSA-2005:061

-Referencia Red Hat: RHSA-2005:330-06

■ MYSQL

MySQL es un servidor de bases de datos multi-usuario y multi-hilo.

Stefano Di Paola descubrió dos errores en la manera en que MySQL maneja fun-

ciones definidas por el usuario. Un usuario con la capacidad de ejecutar funciones definidas por el usuario, podría, potencialmente, ejecutar código arbitrario en el servidor MySQL. El proyecto CVE ha asignado los nombres CAN-2005-0709 y CAN-2005-0710 a estos problemas.

Stefano Di Paola también descubrió un error en la manera en que MySQL crea tablas temporales. Un usuario local podría crear un enlace simbólico manipulado que podría dar como resultado que MySQL sobrescribiera el fichero. El proyecto CVE ha asignado el nombre CAN-2005-0711a este problema. ■

-Referencia Gentoo: GLSA 200503-19 /mysql

-Referencia Mandriva:

MDKSA-2005:060

-Referencia Red Hat: RHSA-2005:334-07

-Referencia Suse: SUSE-SA:2005:019

■ TELNET

El paquete Telnet aporta un cliente telnet desde la línea de comandos. El paquete servidor telnet incluye un demonio telnet, telnetd, que soporta un login remoto a un máquina host. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE – <http://cve.mitre.org>) ha asignado los nombres los nombres CAN-2005-0468 y CAN-2004-0469 a este problema. ■

-Referencia Debian: DSA-703-1krb5

-Referencia Gentoo: GLSA 200504-04 /telnet

-Referencia Red Hat:

RHSA-2005:327-10

■ MOZILLA

Mozilla es un navegador web, cliente de correo y de grupos de noticias, cliente IRC y editor HTML de código abierto.

Se ha descubierto un desbordamiento de búfer en la manera en que Mozilla procesa imágenes GIF. Sería posible para un atacante crear una imagen GIF manipulada que ejecutase código arbitrario cuando fuese visualizado por la víctima. El proyecto CVE ha asignado el nombre CAN-2005-0399 a este problema.

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 propios 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*.

Se descubrió un error en la manera en que Mozilla muestra ventanas de diálogo. Es posible que una página web maliciosa en una pestaña en el fondo presente un diálogo que parezca provenir de la pestaña activa. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2004-1380 a este problema.

Se descubrió un bug en la manera en que Mozilla permitía a plug-ins a cargar contenidos privilegiados en un marco. Es posible que una página web maliciosa pudiera engañar a un usuario para que hiciera clic en ciertos sitios para modificar parámetros de configuración o ejecutar código arbitrario. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2005-0232 a este problema.

Se encontró un error en la manera en que Mozilla Mail maneja cookies cuando se carga correo a través de HTTP, indistintamente de las preferencias del usuario. Es posible que se pudiera trazar a un usuario específico utilizando un mensaje malicioso que cargara contenido a través de HTTP. El proyecto de

Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2005-0149 a este problema.

Se descubrió un error en la manera en que Mozilla responde a peticiones de autenticaciones de proxy. Es posible que un servidor malicioso robe credenciales desde el navegador de una víctima emitiendo una petición 407 de autenticación de proxy. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2005-0147 a este problema.

Otro error se encontró en la manera en que Mozilla maneja ciertas etiquetas de inicio seguidos por un carácter nulo. Una página maliciosa podría hacer que Mozilla se colgara cuando fuese visualizada por la víctima. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2004-1613 a este problema.

Se encontró un error en la manera en la que Mozilla establece permisos al instalar paquetes XPI. Es posible que un XPI instale ficheros con permiso de lectura y escritura globales, permitiendo a un usuario local malicioso robar información o ejecu-

tar código malicioso. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2004-0906 a este problema.

Se descubrió un error en la manera en que Mozilla carga enlaces en las cuales se pulsan con el botón central del ratón en una nueva pestaña. Una página web maliciosa podría leer ficheros locales o modificar parámetros chrom privilegiados. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2005-0141 a este problema.

Se encontró un error en la manera en que Mozilla muestra el icono de sitio seguro. Una página web maliciosa puede utilizar una URL de visualización de código para página segura dirigida a la página segura mientras se carga otra página insegura, mostrándose el icono del estado previo de seguridad. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2005-0144 a este problema. ■

-Referencia Gentoo: GLSA 200503-30 / Mozilla

-Referencia Red Hat: RHSA-2005:323-10

LinuxWorld Conference & Expo – Worldwide Series



LinuxWorld

• Johannesburg:	May 17 – 20, 2005	www.linuxworldexpo.co.za
• Milan:	May 24 – 26, 2005	www.linuxworldexpo.it
• New York:	May 25 – 26, 2005	www.linuxworldexpo.com
• Tokyo:	June 1 – 3, 2005	www.rdg.co.jp/expo/tw/
• San Francisco:	August 9 – 11, 2005	www.linuxworldexpo.com
• Beijing:	August 24 – 26, 2005	www.linuxworldchina.com
• Moscow:	September 7 – 9, 2005	www.linuxworldexpo.ru
• Cape Town:	September 14 – 16, 2005	www.linuxworldexpo.co.za
• London:	October 5 – 6, 2005	www.linuxworldexpo.co.uk
• Utrecht:	November 9 – 10, 2005	www.linuxworldexpo.nl
• Frankfurt:	November 15 – 17, 2005	www.linuxworldexpo.de
• Mexico City:	February 14 – 17, 2006	www.linuxworldexpo.com
• Boston:	April 3 – 6, 2006	www.linuxworldexpo.com



World's Leading Trade Event for Linux and Open Source Businesses

Where open minds meet!