

# Inseguridades

## ■ Cyrus-imapd

El servidor Cyrus IMAP es un servidor de correo electrónico eficiente y altamente escalable. Se han descubierto múltiples vulnerabilidades en los analizadores de argumentos de los comandos *partial* y *fetch* del servidor. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-1012 y CAN-2004-1013 a este problema. También existen problemas de desbordamiento de búfers en el código 'imap magic plus' que son vulnerables de ser explotados (CAN-2004-1011 y CAN-2004-1015).

Un atacante podría explotar estas vulnerabilidades para ejecutar código arbitrario con los permisos del usuario que ejecuta el servidor Cyrus IMAP. No existe ninguna solución por el momento para este problema. Todos los usuarios de Cyrus IMAP deberán actualizar sus servidores a la última versión. ■

-Referencia Debian:

[DSA-597-1 cyrus-imapd](#)

-Referencia Gentoo:

[GLSA 200411-34 /cyrus-imapd](#)

-Referencia Suse: [SUSE-SA:2004:043](#)

## ■ Ruby

Ruby es un lenguaje de scripts interpretado para la creación de programas orientados a objetos de manera fácil y rápida. El módulo CGI de Ruby puede ser utilizado para crear aplicaciones web.

Los desarrolladores de Ruby encontraron y arreglaron un fallo del módulo CGI que permitía su activación remota. Esta vulnerabilidad podía, en teoría, provocar un bucle infinito. Una atacante remoto podría activar la vulnerabilidad a través de una aplicación web Ruby expuesta y provocar que el servidor utilizara recursos de CPU innecesarios, lo que podría causar un ataque por denegación de servicio. Mitre ha asignado el nombre CAN-2004-0983 a este problema.

No existe solución para este problema en el módulo CGI de Ruby. Todos los

usuarios de Ruby 1.6.x deberán actualizar sus versiones. ■

-Referencia Mandrake:

[MDKSA-2004:128](#)

## ■ Kernel

El kernel Linux se encarga de llevar a cabo las funciones básicas del sistema operativo.

Se ha descubierto un fallo de ausencia de serialización en *unix\_dgram\_recvmsg* que afecta a kernels anteriores al 2.4.28. Un usuario local podría potencialmente aprovecharse de una condición de carrera para hacerse con privilegios de root. Se pueden consultar más detalles sobre estos problemas en la base de datos del proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>). Véase CAN-2004-1068.

Paul Starzetz de iSEC descubrió varios fallos en el cargador binario ELF, fallos que afectan a kernels anteriores a 2.4.28. Un usuario local podría utilizar estos fallos para conseguir acceso de lectura a binarios sólo ejecutables o posiblemente conseguir privilegios (CAN-2004-1070, CAN-2004-1071, CAN-2004-1072 y CAN-2004-1073).

Se descubrió un fallo en la configuración de límites TSS que afecta a los kernels para las arquitecturas AMD AMD64 e Intel EM64T anteriores a 2.4.23. Un usuario local podría provocar un ataque de denegación de servicio o cuelgue del sistema o, posiblemente, conseguir privilegios (CAN-2004-0812).

Se ha descubierto un fallo de desbordamiento de entero en la función *ubsec\_keysetup* en el driver Broadcom 5820 cryptonet. En los sistemas que utilicen este driver, un usuario local podría provocar un ataque de denegación de servicio (o cuelgue del sistema) o utilizar el fallo para adquirir privilegios (CAN-2004-0619).

Stefan Esser descubrió varios fallos, incluyendo desbordamientos de búfers en el driver smbfs en kernels anteriores a

2.4.28. Un usuario local podría provocar un ataque de denegación de servicio (cuelgue) o utilizar el fallo para escalar privilegios. Para poder explotar este fallo, el atacante necesitaría tener el control de un servidor Samba (CAN-2004-0883 y CAN-2004-0949).

SGI descubrió un error en el cargador elf que afecta a los kernels anteriores a 2.4.25 que podría activarse con un binario malformado. En arquitecturas diferentes a x86, un usuario local podría crear un binario malicioso que provocara un ataque de denegación de servicio o cuelgue (CAN-2004-0136).

Conectiva descubrió fallos en drivers USB que afectaban los kernels anteriores a 2.4.27 que utilizaban las funciones *copy\_to\_user* en estructuras no inicializadas. Estos fallos podrían permitir a usuarios leer pequeñas cantidades de la memoria del kernel (CAN-2004-0685). ■

-Referencia Red Hat: [RHSA 2004:549-10](#)

-Referencia Suse: [SUSE-SA:2004:042](#)

## ■ Plugin Java de Sun

La seguridad en los entornos del plugin Java de Sun y Blackdown Java puede ser sobreesido para conseguir el acceso a paquetes arbitrarios, lo que permitiría que applets sin confianza llevaran a cabo acciones sin restricciones en sistema huésped.

El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-1012 y CAN-2004-1029 a este problema.

Tanto Sun como Blackdown proporcionan implementaciones del Kit de Desarrollo Java (JDK) y el entorno de ejecución Java (JRE). Ambas implementaciones contienen un plugin Java que permite la ejecución de applets Java en un entorno restringido en navegadores web.

Todos los plugins Java están sujetos a una vulnerabilidad que permite el acceso no restringido a paquetes Java.

Un atacante remoto podría embeber un applet Java malicioso en una página web y engañar a un víctima para que la visualizase. Este applet podría sobreeser las restricciones de seguridad y ejecutar cualquier comando o acceder a cualquier fichero con los permisos del usuario visualizando la página web.

La solución inmediata es deshabilitar los applets Java en los navegadores web. Todos los usuarios de Sun JDK deberán actualizar sus versiones. ■

-Referencia Gentoo:  
GLSA 200411-38/Java

## ■ BNC

BNC es un proxy de devolución de sesiones IRB. Leon Juranic descubrió que BNC no siempre protege a los búfers de la sobrescritura. Esto podía ser explotado por un servidor malicioso IRC para desbordar un búfer de tamaño limitado y ejecutar código arbitrario en el host cliente. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-1052 a este problema. ■

-Referencia Debian: DSA-595-1 bnc  
-Referencia Gentoo: GLSA 200411-24/  
BNC.

## ■ ez-ipupdate

ez-ipupdate es una utilidad para actualizar información de nombres de hosts para un gran número de servicios de DNS dinámicos. Ulf Harnhammar, del Proyecto de Auditorías de Seguridad de Debian, descubrió una vulnerabilidad de formato de cadena en ez-ipupdate. A este problema se le ha asignado el Mitre CVE CAN-2004-0980. ■

-Referencia Debian: DSA-592-1 ez-ipu-  
date  
-Referencia Gentoo: GLSA 200411-20/  
ez-ipupdate

## ■ Samba

Samba es una implementación SMB/CIFS abierto y libre que permite una interoperabilidad sin fisuras de servicios de ficheros e impresión con clientes SMB/CIFS. Se han identificado varias vulnerabilidades en Samba recientemente.

Existe un problema con el demonio del servicio de compartición de ficheros de Samba, el que permite a un usuario remoto hacer que el servicio consuma mucha potencia de computación, lo que podría conllevar potencialmente un cuelgue al consultar nombres de ficheros con comodines especiales.

Este ataque puede tener éxito si el demonio Samba está en ejecución y un

usuario remoto tiene acceso a una compartición (aunque sólo sea en modo lectura). A este problema se le ha asignado el Mitre CVE CAN-2004-0930.

Stefan Esser descubrió un problema en el manejo de cadenas Unicode en el manejo de ficheros Samba que podría conllevar un desbordamiento de pila remoto y podría permitir a usuarios remotos inyectar código en el proceso smbd. A este problema se le ha asignado el Mitre CVE CAN-2004-0882.

Los paquetes actualizados no son vulnerables a estos problemas. Se recomienda que todos los usuarios de Samba se actualicen a la última versión. ■

-Referencia Gentoo: GLSA 200411-21/  
samba  
-Referencia Mandrake:  
MDKSA-2004:136  
-Referencia Red Hat: RHSA-2004:632-17  
-Referencia Suse: SUSE-SA:2004:040.

## ■ sudo

sudo es un programa que aporta privilegios de superusuario limitados a usuarios específicos. Liam Helmer notó que sudo no limpia el entorno lo suficiente. Algunas funciones de bash y la variable CDPATH se siguen pasando al programa en ejecución como usuario privilegiado.

Este hecho deja el sistema vulnerable a la posibilidad de que un atacante pueda encontrar una manera de sobrecargar las rutinas del sistema. A este problema se le ha asignado el Mitre CVE CAN-2004-1051.

Estas vulnerabilidades sólo pueden ser explotadas por usuarios a quienes se les haya otorgado privilegios de superusuario limitados. Se recomienda actualizar los paquetes sudo instalados. ■

-Referencia Debian: DSA-596-2 sudo  
-Referencia Mandrake:  
MDKSA-2004:133

## Políticas de seguridad de la 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 propios sitio web que versa sobre temas relacionadas con la seguridad. Entre otras cosas, incluye de avisos 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 el parche soluciona.

1) Todos los distribuidores muestran correos de seguridad en el campo *Subject*.