

# Inseguridades

## ■ CUPS

El Common UNIX Printing System (CUPS) es un sistema de impresión. Álvaro Martínez Echevarría informó de un error en la versión del Protocolo de Impresión de Internet (Internet Printing Protocol o IPP) en versiones de CUPS anteriores a 1.1.21. Un atacante podría enviar un paquete cuidadosamente escrito al puerto IPP, lo que podría provocar que CUPS dejara de escuchar en ese puerto y desencadenar un ataque de denegación de servicio. Para poder explotar este error, un atacante tendría que tener la capacidad de enviar un paquete UDP al puerto IPP (por defecto,

631). El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-0558 a este problema. ■

*Referencia Debian: DSA-545-1*

*Referencia Gentoo: GLSA 200410-06/cups*

*Referencia Mandrake: MDKSA-2004:097*

*Referencia Red Hat: RHSA-2004:449-17*

*Referencia Slackware: SSA:2004-266-01*

*Referencia Suse: SUSE-SA:2004:031*

## ■ getmail

getmail es un sustituto fiable de fetchmail que soporta Maildir, Mboxrd y envío de MDAs externos. David Watson descubrió

una vulnerabilidad en getmail cuando se configura para correr como root y envía correo a ficheros maildir/mbox de usuarios locales no de confianza. Un usuario local malicioso podría explotar una condición de carrera, o un ataque symlink similar y dotar a getmail con la capacidad de crear o sobrescribir ficheros en cualquier directorio en el sistema. No se debe ejecutar getmail como usuario privilegiado ni, en la versión 4, utilizar un MDA externo con privilegios de usuarios y grupos explícitamente configurados. Todos los usuarios de getmail deben actualizar a la última versión. ■

*Referencia Debian: DSA-553-1*

*Referencia Gentoo: GLSA 200409-32/getmail*

*Referencia Slackware: SSA:2004-278-01*

## ■ Mozilla

Mozilla es un navegador web de código abierto, un cliente de correo y grupos de noticias avanzado, cliente IRC y editor de HTML. Se han descubierto recientemente varios errores en la suite. Jesse Ruderman descubrió un error de scripting multidominio en Mozilla. Si a un usuario se le engaña para que arrastre un enlace de Javascript hasta otro marco o página, se dota al atacante de la capacidad de hurtar o modificar información sensible de ese sitio. Además, si a un usuario se le engaña para que arrastre secuencialmente dos enlaces a otra ventana (no marco), se le dota al atacante de la capacidad de ejecutar comandos arbitrarios. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-0905 a este problema. Gael Delalleau ha descubierto un desbordamiento de entero que afecta le código que maneja BMP dentro de Mozilla. Un atacante podría utilizar un fichero BMP cuidadosamente manipulado para provocar un cuelgue del programa o que ejecute código arbitrario cuando se visualizase el archivo. El CVE ha asignado el nombre CAN-2004-0905 a este problema. Georgi Guninski ha descubierto un desbordamiento de búfer basado en pila en las rutinas de muestra de vCard. Un atacante podría crear un vCard cuidadosamente manipulado que podría hacer que Mozilla se cuelgue o ejecute código arbitrario cuando se muestra. El mismo

## 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*.

autor ha descubierto otro desbordamiento de búfer basado en pila en el módulo de "Envío de Página". El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-0902 a este problema. Wladimir Palant ha descubierto un fallo en la manera en que Javascript interactúa con el portapapeles. Un atacante tiene la posibilidad de utilizar código malicioso de Javascript para robar datos sensibles que han sido copiados al portapapeles. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-0908 a este problema. ■

*Referencia Red Hat: RHSA-2004:486-18*

*Referencia Slackware: SSA:2004-266-03*

*Referencia Suse: SUSE-SA:2004:036*

## ■ gtk+

El paquete gtk2 contiene el kit de herramientas de *the GIMP* (GTK+), una librería para la creación de interfaces gráficas de usuario para el sistema de ventanas X. Durante las pruebas de un fallo anteriormente corregido en QT (CAN-2004-0691), se descubrió un error en el procesador de imágenes BMP de gtk2. Un atacante podría crear un fichero BMP cuidadosamente manipulado que podría provocar que una aplicación entrase en un bucle infinito y no respondiese a las entradas del usuario cuando fuese abierto por la víctima. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-0753 a este problema. Durante una auditoría de seguridad, Chris Evans descubrió un desbordamiento de pila en el decodificador de imágenes XPM. Un atacante podría crear un fichero XPM cuidadosamente manipulado que podría hacer que una aplicación enlazada con gtk2 se cuelgue o posiblemente ejecute código arbitrario cuando la víctima abra el fichero. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado los nombres CAN-2004-0782 y CAN-2004-0783 a este problema. El mismo autor

también descubrió un desbordamiento de entero en el decodificador de imágenes ICO. Un atacante podría crear un fichero ICO cuidadosamente manipulado que hiciera que una aplicación enlazada con gtk2 se cuelgue cuando la víctima abriese el fichero (CAN-2004-0788). ■

*Referencia Debian: DSA-549-1*

*Referencia Red Hat: RHSA-2004:466-12*

*Referencia Slackware: SSA:2004-266-02*

*Referencia Suse: SUSE-SA:2004:033*

## ■ OpenOffice.org

OpenOffice.org es un conjunto de aplicaciones para la productividad ofimática que incluye programas de escritorio, como procesadores de texto, hoja de cálculo, administrador de presentaciones, editor de fórmulas y un programa de diseño. La empresa Secunia Research informó de un problema derivado de la manipulación de ficheros temporales en OpenOffice.org. Un usuario local malicioso podría utilizar este fallo para acceder a los contenidos de los documentos abiertos de otro usuario. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-0752 a este problema. Se aconseja a todos los usuarios de OpenOffice.org que actualicen sus programas con los paquetes de actualización de OpenOffice.org que contienen un parche retroactivo para corregir este problema. ■

*Referencia Mandrake: MDKSA-2004:103*

*Referencia Red Hat: RHSA-2004:446-08*

## ■ SpamAssassin

SpamAssassin aporta maneras de reducir correos electrónicos comerciales no solicitados (SPAM) en las bandejas de correo entrante. Se ha encontrado un error de denegación de servicio en versiones inferiores a 2.64. Un atacante malicioso podría crear un mensaje de tal modo que provocaría que SpamAssassin dejara de responder. Este ataque de denegación de servicio podría provocar que SpamAssassin deje de remitir y filtrar correo. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-0796 a este problema. Los usuarios de SpamAssassin deberán actu-

alizar sus sistemas para incluir los paquetes nuevos que solucionan este problema. Los nuevos paquetes contienen un parche retroactivo que no es vulnerable a este tipo de ataques de denegación de servicio. ■

*Referencia Red Hat: RHSA-2004:451-05*

## ■ XFree86

XFree86 es una implementación de código abierto del sistema de ventanas X. Aporta una funcionalidad básica de bajo nivel para la que están diseñadas las interfaces gráficas de usuario (GUIs) completos tales como Gnome o KDE. Durante una auditoría de código fuente, Chris Evans descubrió varios fallos de desbordamientos de pila y un desbordamiento de entero en la librería *libXpm* de X.org utilizada para decodificar imágenes XPM (X PixMap). Un atacante que supiera aprovechar este problema, podría crear un fichero XPM cuidadosamente manipulado que haría que una aplicación enlazada con la mencionada librería se colgase y ejecutase código arbitrario si el fichero es abierto por la víctima. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado los nombres CAN-2004-0687, CAN-2004-0688 y CAN-2004-0692 a estos problemas de seguridad de XFree86. Se descubrió un fallo en el X Display Manager (XDM). XDM abría un socket TCP *chooserFd*, aún si el parámetro *DisplayManager.requestPort* estuviera establecido como 0. El efecto de esta situación es que permitía el acceso de usuarios autorizados al ordenador a través de X, aún si el administrador del ordenador hubiera configurado XDM para rechazar conexiones. Aunque XFree86 versión 4.3.0 no era vulnerable a este problema, Red Hat Enterprise Linux 3 contenía un parche retroactivo que introducía el error. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-0419 a este problema. ■

*Referencia Debian: DSA-561-1*

*Referencia Gentoo: GLSA 200409-34/X*

*Referencia Mandrake: MDKSA-2004:099*

*Referencia Red Hat: RHSA-2004:478-13*

*Referencia Suse: SUSE-SA:2004:034*