

INSEGURIDADES

■ OPENOFFICE.ORG

OpenOffice.org es una suite ofimática orientada a la productividad que incluye aplicaciones de escritorio tales como un procesador de textos, hoja de cálculo, administrador de presentaciones, editor de fórmulas y un programa de diseño vectorial.

Se ha encontrado un error de desbordamiento de búfer basado en pila en el procesador de ficheros DOC de OpenOffice. Un atacante que conociera este error, podría crear un fichero DOC cuidadosamente manipulado que provocara que OpenOffice ejecutara código arbitrario cuando el fichero se abriera por parte de la víctima.

El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE – <http://cve.mitre.org>) ha asignado el nombre CAN-2005-0941 a este problema.

Se recomienda a todos los usuarios de OpenOffice que se actualicen a la última versión. ■

-Referencia Gentoo: GLSA 200504-13 /

OpenOffice

-Referencia Mandriva:

MDKSA-2005:082

-Referencia Red Hat: RHSA-2005:375-07

-Referencia Suse: SUSE-SA:2005:025

■ ETHEREAL

Ethereal es un analizador de protocolos de red de múltiples características. Algunos investigadores han descubierto recientemente numerosas vulnerabilidades en versiones de Ethereal anteriores a la versión 0.10.11. Estas vulnerabilidades incluyen problemas como los siguientes:

- Los dissectores de ANSI A y DHCP son vulnerables a vulnerabilidades de formato de cadenas.

- Los dissectores de DISTCC, FCELS, SIP, ISIS, CMIP, CMP, CMS, CRMF, ESS, OCSP, PKIX1 Explicit, PKIX Qualified, X, 509, Q.931, MEGACO, NCP, ISUP, TCAP y Presentation son vulnerables a desbordamientos de búfers.
- Los dissectores de KINK, WSP, SMB Mailslot, H.245, MGCP, Q.931, RPC, GSM, y SMB NETLOGON son vulnerables a errores de manejo de punteros.
- Los dissectores LMP, KINK, MGCP, RSVP, SRVLOC, EIGRP, MEGACO, DLSw, NCP y L2TP son vulnerables a problemas de bucles.
- Los dissectores Telnet y DHCP pueden llegar a abortar.
- Los dissectores TZSP, Bittorrent, SMB, MGCP y ISUP pueden provocar un fallo de segmentación.

LinuxWorld Conference & Expo – Worldwide Series



LinuxWorld

- | | | |
|------------------|-------------------------|--|
| • San Francisco: | August 8 – 11, 2005 | www.linuxworldexpo.com |
| • Beijing: | August 17 – 19, 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 |
| • Sydney: | March 28 – 30, 2006 | www.linuxworldexpo.com |
| • Boston: | April 3 – 6, 2006 | www.linuxworldexpo.com |
| • Milan: | April 12 – 14, 2006 | www.linuxworldexpo.it |



World's leading Trade Event for Linux and Open Source in business

Where open minds meet!

- Los disectores GSM MAP, AIM, Fibre Channel, SRVLOC, NDPS, LDAP, y NTLMSSP podrían terminar de manera anormal.

Un atacante podría utilizar estas vulnerabilidades para colgar Etherreal y ejecutar código arbitrario con los permisos del usuario que corre Etherreal, que podría ser el usuario root. Esto podría comprometer la seguridad del sistema a conllevar el escalado de privilegios. ■

-Referencia Debian: DSA-718-2 etherreal

-Referencia Gentoo: GLSA 200505-03 / Etherreal

-Referencia Mandriva:

MDKSA-2005:083

■ FIREFOX

Firefox es un navegador web de código abierto.

Vladimir V. Pereplitsa descubrió un error en la manera en que Firefox utiliza funciones anónimas durante el reemplazo de cadenas de expresiones regulares.

Esto posibilita que una página web maliciosa capture un bloque arbitrario de memoria del navegador. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2005-0989 a este problema.

Omar Khan descubrió un error en la manera en que Firefox procesa la etiqueta PLUGINSFRAME. Una página web maliciosa puede engañar a un usuario y hacer que pulse el botón de "Instalación manual" para que instale un plugin desconocido. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2005-0752 a este problema.

Doron Rosenberg descubrió un error en la manera en que Firefox muestra una ventana emergente. Si un usuario elige abrir una ventana emergente cuya URL es un guión JavaScript malicioso, el guión se ejecutará con privilegios elevados. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el

nombre CAN-2005-1153 a este problema.

Se encontró un error en la manera en que Firefox maneja el rango global javascript para una ventana. Una página web maliciosa podría definir una variable global que se supiera que se utiliza en otro sitio web, permitiendo al código malicioso ejecutarse en el contexto de ese sitio. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2004-1154 a este problema.

Michael Krax descubrió un error en la manera en que Firefox instala plugins de búsqueda. Si un usuario escoge instalar un plugin de búsqueda desde un sitio malicioso, éste podría sobrescribir silenciosamente un plugin existente. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado los nombres CAN-2005-1156 y CAN-2005-1157 a este problema.

Kohei Yoshino descubrió un error en la manera en que Firefox abre enlaces en el panel lateral. Una página web maliciosa. Podría construir un enlace de tal manera que, cuando un usuario hiciera clic en él, podría ejecutar javascript arbitrario con privilegios elevados. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2005-1158 a este problema.

Se encontró un error en la manera en que Firefox valida varios objetos XPInstall relacionados con javascript. Una página web maliciosa podría pasar otros objetos a los objetos XPInstall, lo que resultaría en que el intérprete javascript saltaría a localizaciones arbitrarias en memoria. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2005-1159 a este problema.

Se encontró un error en la manera en que el código UI privilegiado maneja nodos DOM. Una página web maliciosa podría instalar código javascript malicioso o robar datos. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2005-1160 a este problema. ■

-Referencia Gentoo: GLSA 200504-18 /

Mozilla; GLSA 200505-11 / mozilla

-Referencia Mandriva:

MDKSA-2005:088

-Referencia Red Hat: RHSA-2005:323-07

-Referencia Slackware:

SSA:2005-111-04; SSA:2005-135-01

-Referencia Suse: SUSE-SA:2005:028

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*.