

INSEGURIDADES

■ PHP

PHP es un lenguaje de scripting embebido en HTML usado frecuentemente con el servidor Web HTTP de Apache.

La función `phpinfo()` de PHP no sanitiza adecuadamente las cadenas largas. Un atacante podría usar esto para llevar a cabo ataques de scripting multisitio contra sitios que tienen scripts PHP disponibles públicamente y que llaman `phpinfo()`. (CVE-2006-0996).

Se ha encontrado que la función PHP `html_entity_decode()` no es segura a nivel

binario. Un atacante podría usar este fallo para revelar una parte de la memoria del servidor atacado. Con objeto de que este problema sea explotable, el sitio de destino necesitaría tener un script PHP que llamara a la función `html_entity_decode()` con una entrada que no filtrase por confianza del usuario y presentara los resultados. (CVE-2006-1490).

Se ha encontrado que la salida de error de PHP no escapa correctamente HTML en algunos casos. Un atacante podría usar este fallo para realizar ataques de scripting

multisitio contra sitios donde están habilitados tanto `display_errors` como `html_errors`. (CVE-2006-0208).

Se ha encontrado un error en la validación de la entrada en la función `"mb_send_mail()"`. Un atacante podría usar este fallo para inyectar cabeceras arbitrarias en un correo enviado vía script llamando a la función `"mb_send_mail()"` donde el parámetro `"To"` puede ser controlado por el atacante. (CVE-2005-3883).

Se descubrió un fallo de desbordamiento de búfer en `uw_imap`, el Servidor IMAP de la Universidad de Washington. `php-imap` está compilado contra las librerías de `c-client` estáticas desde `imap` y además necesita ser recompilada contra la versión fijada. ■

Referencia Gentoo: GLSA-200605-08

Referencia Mandriva: MDKSA-2006:074

Referencia Red Hat: RHSA-2006:0276-9

Referencia Suse: SUSE-SA:2006:024

■ Xorg-X11

Xorg es una implementación de código abierto de un sistema X Window. Proporciona la funcionalidad de bajo nivel básica de las que hacen uso interfaces de usuario gráficas como GNOME y KDE.

Se ha descubierto un fallo de desbordamiento de búfer en la extensión `RENDER` del servidor Xorg. Un cliente autorizado malicioso podría explotar este problema y causar una denegación de servicio (colgar el sistema) o ejecutar código arbitrario potencialmente con privilegios de superusuario en el servidor Xorg. (CVE-2006_1526). ■

Referencia Gentoo: GLSA-200605-02

Referencia Mandriva: MDKSA-2006:081

Referencia Red Hat: RHSA-2006:0451-9

Referencia Slackware: SSA:2006-123-01

Referencia Suse: SUSE-SA:2006:023

■ ClamAV

ClamAV es un escáner de virus con licencia GPL.

ClamAV contiene vulnerabilidades de formato código de registro (CVE-2006-1615).

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 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*.

Además, Damian Put descubrió un desbordamiento de número entero en el analizador cabeceras de PE de ClamAV (CVE-2006-1614) y David Luyer descubrió que ClamAV puede ser inducido fraudulentamente a que lleve a cabo un acceso de memoria inválido. (CVE-2006-1630).

Mediante el envío por correo de un adjunto malicioso a un servidor de correo ejecutando ClamAV, un atacante remoto podría causar una Denegación de Servicio o la ejecución de código arbitrario. Obsérvese que el desbordamiento en el analizador del encabezamiento PE solamente es explotable cuando se encuentra deshabilitada la opción Archive-MaxFileSize.

Ulf Härnhammar y un investigador anónimo alemán descubrieron una vulnerabilidad en el código del protocolo de freshclam, una utilidad de la línea de comandos responsable de la descarga e instalación de las actualizaciones de las firmas de virus para ClamAV. Esto podría llevar a una denegación de servicio o potencialmente a la ejecución de código arbitrario. ■

Referencia Debian: DSA-1050-1

Referencia Gentoo: GLSA 200604-06, GLSA 200605-03

Referencia Mandriva:MDKSA-2006:080

Referencia Suse: SUSE-SA:2006:020

■ Mozilla, Firefox y Thunderbird

Mozilla es un navegador web de código abierto, cliente de correo, cliente de grupos de noticias, cliente de chat IRC y editor HTML. Mozilla Firefox es un navegador web de código abierto. Mozilla Thunderbird es un cliente de correo electrónico y de grupos de noticias independiente.

Los expertos han encontrado varios problemas de seguridad relacionados con la suite de Mozilla. Estos problemas también se aplican a herramientas tales como al navegador Firefox y al cliente de correo Thunderbird, basados ambos en Mozilla.

Se han encontrado algunos fallos en la manera en la que Mozilla procesa código javascript malformado. Una página web maliciosa podría modificar el contenido de una página web abierta diferente, posiblemente robando información sensible o iniciando un ataque de scripting multisitio. (CVE-2006-1731, CVE-2006-1732, CVE-2006-1741).

Han sido encontrados algunos errores en la manera en la que Mozilla procesa ciertos fragmentos de javascript. Una página web maliciosa podría ejecutar instrucciones javascript arbitrarias con los permisos de "chrome", permitiendo que la página robe información sensible o instale software dañino. (CVE-2006-1727, CVE-2006-1728, CVE-2006-1733, CVE-2006-1734, CVE-2006-1735, CVE-2006-1742).

Se han encontrado algunos fallos en la manera en la que Mozilla procesa páginas web malformadas. Un atacante, con una página web maliciosamente manipulada, podría causar la ejecución de código arbitrario con los privilegios del usuario ejecutando Mozilla. (CVE_2006-0748, CVE_2006-0749, CVE_2006-1730, CVE-2006-1737, CVE_2006-1738, CVE-2006-1739, CVE-2006-1790).

Se ha encontrado un error en la manera en la que Mozilla presenta el icono del sitio seguro. Si un navegador se configura para presentar por defecto el diálogo de aviso modal de sitio seguro, puede ser posible engañar al usuario haciéndole creer que está viendo un sitio seguro. (CVE-2006-1740).

Se ha encontrado un fallo en la manera en la que Mozilla permite eventos de mutación javascript en elementos de entrada de formularios. Se podría crear una página web maliciosa de tal modo que cuando un usuario presenta un formulario, un fichero arbitrario podría ser cargado por el atacante. (CVE_2006-1729).

Se ha encontrado un fallo en la manera en la que Mozilla ejecuta el reenvío de correo en línea. Si un atacante puede inducir a un usuario a que mande en línea un mensaje de correo maliciosamente manipulado, es posible que el mensaje ejecute javascript con los permisos de "chrome". (VCVE_2006-0884). ■

Referencia Debian: DSA-1046-1

Referencia Gentoo: GLSA-200605-09

Referencia Mandriva: MDKSA-2006:075, MDKSA-2006:078

Referencia Red Hat: RHSA-2006:0328-15, RHSA-2006:0329-13, RHSA-2006:0330-15

Referencia Slackware: SSA:2006-120-01

Referencia Suse: SUSE-SA:2006:021, SUSE-SA:2006:022

■ Kernel Linux

El kernel Linux maneja las funciones básicas del sistema operativo. Informes recientes han puesto de manifiesto los siguientes problemas:

- Un fallo en la implementación IPv6 permite a un usuario local causar una denegación de servicio (bucles infinitos y cuelgues) (CVE-2005-2973, importante)
- un fallo en la implementación puente permite a un usuario remoto causar el envío de paquetes spoof a través envenenamiento de la tabla de envío con frames caídos previamente. (CVE-2005-3272, moderado)
- un fallo en el módulo atm permite a un usuario local causar una denegación de servicio (pánico) a través ciertas llamadas a socket (CVE-2005-3359, importante)
- un fallo en la implementación del cliente NFS permite a un usuario local causar una denegación de servicio (pánico) a través de escrituras O-DIRECT (CVE-2006-0555, importante)
- una diferencia en la operación "sysretq" de los procesadores EM64T (a diferencia de lo que ocurre en los Opteron) permite a un usuario local causar una denegación de servicio (el sistema se cae) con el retorno de ciertas llamadas del sistema (CVE-2006-0741 y CVE-2006-0744, importante)
- un fallo en la implementación keyring permite a un usuario local causar una denegación de servicio (OOPS) (CVE-2006-1522, importante)
- un fallo en la implementación enrutado IP permite a un usuario local causar una denegación de servicio (pánico) a través de una petición para una ruta para una IP multicast (CVE-2006-1525, importante)
- un fallo en la implementación SCTP-netfilter permite a un usuario remoto causar una denegación de servicio (bucle infinito) (CVE-2006-1527, importante)
- un fallo en el driver sg permite a un usuario local causar una denegación de servicio (el sistema se culega) a través una transferencia dio a espacio E/S de memoria mapeada (nmap) (CVE-2006-1528, importante) ■

Referencia Red Hat: RHSA-2006:0493-6