

Inseguridades

■ PHP

PHP es un lenguaje de guiones embebido en HTML que habitualmente se utiliza en conjunción con el servidor web Apache.

Existen fallos encontrados en el código de deserialización de PHP que podrían conllevar al revelado de información, subflujo de matriz de referencia a índice negativa o sin doble. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-1019 a este problema.

También se ha encontrado un fallo en la extensión exif de PHP que podría desembocar en un desbordamiento de pila. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2004-1065 a este problema.

Asimismo, se descubrió un error de revelado de información en el proceso de análisis variables "GPC" en PHP (cadenas de consultas o cookies y datos de formularios POST). Si algún script en particular utilizara los valores de las variables GPC, se podrían revelar porciones del espacio de memoria del proceso httpd hijo al cliente. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2004-0958 a este problema.

Se reveló un error en el análisis de formularios "datos de formulario/multi-parte" utilizado por guiones PHP que permiten subir ficheros a la web. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2004-0959 a este problema.

Se encontraron fallos en las funciones PHP shmop_write, pack y unpack. Estas funciones no suelen recibir información aportada por el usuario, por tanto requerirían un guión PHP malicioso para su explotación. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2004-1018 a este problema.

Existen varios problemas relacionados con el uso de la llamada al sistema

"select" de PHP, que podría desencadenarse si se utiliza en una configuración con Apache.

El script del shell "phpsize", incluido con PHP, puede utilizarse para construir módulos de extensiones de terceras partes. Se encontró un problema de construcción en el script "phpsize" en ciertas plataformas de 64 bits que impedía su correcta operación.

El módulo de extensión "pcntl" se encuentra ahora habilitado en el intérprete de la línea de comandos de PHP (/usr/bin/php). Este módulo permite controlar características tales como "fork" y "kill" desde guiones PHP. ■

-Referencia Gentoo: GLSA 200412-14 / PHP

-Referencia Red Hat: RHSA:2004:687-05

■ Samba

Samba aporta servicios de compartición de ficheros e impresión a clientes SMB/CIFS.

Greg MacManus, de los laboratorios iDEFENSE, ha descubierto un error de desbordamiento de entero en versiones de Samba anteriores a 3.0.10. Un usuario autenticado remotamente podría explotar este error, lo que podría llevar a la ejecución de código arbitrario en el servidor Samba. El proyecto de Vulnerabilidades y Exposiciones Comunes (cve.mitre.org) ha asignado el nombre CAN-2004-1154 a este problema.

Los usuarios de Samba deberán instalar actualizaciones cuanto antes. ■

-Referencia Gentoo: GLSA 200412-13 / Samba

-Referencia Mandrake:

MDKSA-2004:158

-Referencia Red Hat: RHSA:2004:670-10

-Referencia Suse: SUSE-SA:2004:045

■ ZIP

El programa Zip es una utilidad de archivado que puede crear archivos compatibles con ZIP.

Se ha descubierto un error de desbordamiento de búfer en zip cuando maneja nombres de archivos largos. Un atacante podría crear un nombre de accesos espe-

cialmente configurado que podría provocar el cuelgue de zip o que ejecutara instrucciones arbitrarias. El proyecto de Vulnerabilidades y Exposiciones Comunes (<http://cve.mitre.org>) ha asignado el nombre CAN-2004-1010 a este problema. ■

-Referencia Debian: DSA-624-1

-Referencia Red Hat:

RHSA:2004:634-08.

■ nfs-utils

El paquete nfs-utils suministra un demonio para el servidor NFS del kernel y herramientas relacionadas, lo que aporta un nivel más alto de rendimiento que el servidor NFS tradicional de Linux utilizado por la mayoría de los usuarios.

Este paquete también incluye el programa showmount. Este programa consulta al demonio de montaje en un host remoto para recoger información sobre el servidor NFS.

SGI informa que el demonio statd no manejaba correctamente la señal SIGPIPE. Un par incorrectamente configurado o malicioso podría provocar el cuelgue de statd, lo que conllevaría un denegación de servicio. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2004-1014 a este problema.

Arjan van de Ven descubrió un desbordamiento de búfer en rquotad. En arquitecturas de 64 bits, una conversión inadecuada de enteros puede causar este desbordamiento. El proyecto de Vulnerabilidades y Exposiciones Comunes ha asignado el nombre CAN-2004-0946 a este problema. ■

-Referencia Gentoo: GLSA 200412-08

/ nfs-utils

-Referencia Red Hat: RHSA:2004:583-09

■ Kernel

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

Este aviso incluye parches para varios problemas de seguridad:

Petr Vandrovec descubrió un fallo en el código de emulación de 32 bits que afecta al kernel 2.4 de Linux en la arquitectura AMD64. Un atacante local podría utilizar este fallo para escalar privilegios. El proyecto de Vulnerabilidades y Exposiciones Comunes ([6](http://</p>
</div>
<div data-bbox=)

cve.mitre.org) ha asignado el nombre CAN-2004-1144 a este problema.

ISEC Security Research descubrió múltiples vulnerabilidades en la funcionalidad IGMP, que se retro-portó en los kernels Red Hat Enterprise Linux 3. Estos fallos podrían permitir a un usuario local provocar una denegación de servicio (cuelgue) o, potencialmente, servir para escalar privilegios en el sistema. En el caso de utilizarse aplicaciones multicast en el sistema, estos fallos también podrían permitir a un usuario remoto provocar un ataque de denegación de servicio. El proyecto de Vulnerabilidades y Exposiciones Comunes (<http://cve.mitre.org>) ha asignado el nombre CAN-2004-1137 a este problema.

ISEC Security Research y Georgi Guninski descubrieron independientemente un fallo en la función `scm_send` en la capa de mensajes auxiliares. Un usuario local podría crear un mensaje auxiliar cuidadosamente manipulado que provocaría una denegación de servicio (cuelgue del sistema). El proyecto de Vulnerabilidades y Exposiciones Comunes (<http://cve.mitre.org>) ha asignado el nombre CAN-2004-1016 a este problema.

Se ha descubierto una fuga de información de punto flotante en el código de intercambio de contexto de la arquitectura ia64. Un usuario local podría utilizar este fallo para leer los valores de registro de otros procesos, estableciendo el bit MFH. El proyecto de Vulnerabilidades y Exposiciones Comunes (<http://cve.mitre.org>) ha asignado el nombre CAN-2004-0565 a este problema.

Kirill Korotaev encontró un fallo en el binario `load_elf_binary` que afecta los kernels anteriores a 2.4.26. Un usuario local podría utilizar este fallo para crear un binario cuidadosamente manipulado de tal manera que provocase una denegación de servicio (cuelgue del sistema). El proyecto de Vulnerabilidades y Exposiciones Comunes (<http://cve.mitre.org>) ha asignado el nombre CAN-2004-1234 a este problema. ■

-Referencia Red Hat: RHSA:2004:689-06

-Referencia Suse: SUSE-SA:2004:044

■ Acrobat

Acrobat Reader de Adobe es una aplicación de escritorio que permite la vi-

sualización, distribución e impresión de documentos en el formato de portable document format (PDF).

IDEFENSE ha informado que Adobe Acrobat Reader 5.0 aporta un potencial desbordamiento de búfer cuando decodifica documentos codificados con uuencode. El proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado el nombre CAN-2004-0631 a este problema.

Se aconseja a todos los usuarios de Acrobat Reader que se actualicen a las nuevas versiones. ■

-Referencia Red Hat: RHSA:2004:432-08

■ PNG

Se han descubierto varias vulnerabilidades en la librería PNG, utilizada por aplicaciones que soportan el formato de imágenes PNG.

Es posible provocar un desbordamiento a través de características relacionadas con el comportamiento de la librería PNG en aplicaciones de procesamiento de aplicaciones (VU#388984, VU#3817368, CAN-2004-0597). Un atacante podría utilizar un tipo especial de imagen PNG para provocar el cuelgue de una aplicación debido a una desreferencia a puntero nulo en la función `png_handle_iCPP()` (y otras - VU#236656, CAN-2004-0598). Se han descubierto algunos desbordamientos de enteros en las funciones `png_handle_sPLT()`, `png_read_png()` y otras. Estos errores pueden provocar cuelgues en aplicaciones (VU#160448, VU#477512, VU#286464, CAN-2004-0599). ■

-Referencia SuSE: SUSE-SA:2004:023

-Referencia Slackware:

SSA:2004-222-01

Políticas de seguridad de la 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*.