

INSEGURIDADES

■ sponly

El paquete sponly es una shell restringida que permite unos pocos comandos predefinidos. A menudo se usa como un complemento a OpenSSH para proporcionar el acceso a usuarios remotos sin la necesidad de cesión de privilegios remotos.

Max Vozeler descubrió que el comando *sponly* permite a los usuarios crear un entorno chroot en directorios arbitrarios. Además, Pekka

Pessi informó acerca de otro problema de seguridad: sponly validaba insuficientemente los parámetros de la línea de comandos a scp o al comando rsync.

Un atacante local podría obtener privilegios de superusuario mediante un chroot a directorios arbitrarios que contengan enlaces duros a programas setuid. Un usuario remoto de sponly también podría enviar parámetros maliciosos a scp o al comando rsync que

le permitirían eludir las restricciones de la shell y ejecutar programas arbitrarios. ■

Referencia Gentoo: GLSA-200512-17

■ Apache

El Servidor HTTP Apache es un servidor de web popular y libremente disponible.

Una fuga de memoria en de la versión worker MPM permitiría que atacantes remotos causaran una denegación de servicio (consumo de memoria) mediante conexiones abortadas. El Proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE – <http://cve.mitre.org>) ha asignado a este problema el nombre CVE-2005-2970. Esta vulnerabilidad sólo afecta a los usuarios que están usando la versión worker MPM no predeterminado.

Se descubrió un fallo en el módulo mod_imap en el uso de la directiva Referer con mapas de imágenes. Con determinadas configuraciones del sitio, un atacante remoto podría realizar un ataque de scripting multisitio si la víctima es forzada a realizar una visita a una URL maliciosa usando determinados buscadores de web. (CVE-2005-3352)

Se descubrió un fallo de puntero NULL en mod_ssl que afectaba a las configuraciones de servidores donde un host virtual SSL es configurado con un acceso de control y un documento cliente de error 400. Este fallo se traduciría sólo en una denegación de servicio si se usa la versión worker MPM no predeterminado. (CVE-2005-3357) ■

Referencia Mandriva: MDKSA-2006:007

Referencia Red Hat: RHSA-2006:0159

■ xpdf,gpdf,kpdf

xpdf,gpdf y kpdf son visores para ficheros PDF (Portable Document Format).

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*.

Se han descubierto algunos fallos en estos visores de PDFs. Un atacante podría construir un fichero PDF cuidadosamente manipulado que haría posible que el visor se colgara o que posiblemente ejecutara código arbitrario cuando se abriera. El Proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado a estos problemas los nombres CVE-2005-3191, CVE-2005-3192 y CVE-2005-3191. ■

Referencia Gentoo: GLSA-200512-08
Referencia Red Hat: RHSA-2005:867

■ **CUPS**

El Common UNIX Printing System (CUPS) proporciona una capa de impresión portable para sistemas UNIX y Linux.

Se descubrieron algunos errores en la manera en la que CUPS procesa los PDFs. Un atacante podría construir un PDF haciendo que CUPS se colgara o

que posiblemente ejecutara código arbitrario. El Proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE - <http://cve.mitre.org>) ha asignado a estos problemas los nombres CVE-2005-3191, CVE-2005-3192 y CVE-2005-3191. ■

Referencia Red Hat: RHSA-2005:878

■ **cURL**

cURL es una herramienta para la obtención de ficheros de servidores FTP, HTTP, Gopher, Telnet y Dict usando cualquiera de los protocolos soportados.

Stefan Esser descubrió un error off-by-one en un bucle. Es posible ejecutar código arbitrario sobre la máquina de un usuario si éste consigue que se ejecute un bucle con una URL cuidadosamente manipulada. El Proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE -

<http://cve.mitre.org>) ha asignado a este problema el nombre CVE-2005-4077. ■

Referencia Debian: DSA-919-1 curl
Referencia Gentoo: GLSA-200512-09
Referencia Mandriva: MDKSA-2005:224
Referencia Red Hat: RHSA-2005:875

■ **VMware Workstation**

VMware Workstation es una potente máquina virtual para desarrolladores y administradores de sistemas.

Tim Shelton descubrió que vmnetnatd, el módulo host que proporciona la red estilo BAT para sistemas operativos huéspedes de VMware es incapaz de procesar peticiones EPRT y PORT FTP incorrectas.

Usuarios de sistemas operativos huéspedes maliciosos que usan la red NAT o Workstation VMware locales podrían explotar esta vulnerabilidad para ejecutar código arbitrario en el sistema host con privilegios elevados. ■

Referencia Gentoo: GLSA-200601-04

Descubre lo que te espera en la Red

Zona de descarga

Servicio al lector

Artículos descargables

Calendario de eventos

