

# INSEGURIDADES

## lighttpd

Lighttpd es un servidor web ligero para usuarios que no necesitan las características de Apache ni sus importantes consumos de memoria. Se han descubierto cuatro problemas. Dos de ellos corresponden a problemas de ataque de denegaciones de servicio que se aplican a lighttpd ejecutándose en casi cualquier plataforma que podrían permitir situaciones de denegación de servicio. (CVE-2007-3946, CVE-3947)

La tercera cuestión es un problema en `mod_access` que permitiría que un usuario remoto evitara restricciones de acceso.

El cuarto tema se refiere también a una denegación de servicio para máquinas ejecutando lighttpd en plataformas de 32 bits. (CVE-2007-3949, CVE-3950) ■

*Referencia Debian: LSA 1362-1*

*Referencia Gentoo: GLSA-200708-11*

*Referencia SUSE: SUSE-SR:2007:015*

## postfix-policyd

Postfix-policyd es un paquete anti-spam para el popular programa de manipulación de correo Postfix.

Debido a un error en la manera en la que el límite de postfix-policyd comprueba los paquetes de SMTP entrantes, paquetes malformados podrían desencadenar la explotación remota de código arbitrario. (CVE-2007-3791) ■

*Referencia Debian: DSA-1361*

## rsync

Rsync es un programa para realizar copias remotas a alta velocidad. Debido a un problema de desbordamiento de búfer, un atacante remoto podría usar nombres extensos de directorios para ejecutar código arbitrario. (CVE-2007-4091) ■

*Referencia Debian: DSA-1360*

*Referencia SUSE: SUSE-SR:2007:017*

*Referencia Ubuntu: USN-500-1*

## xpdf

Xpdf es un visor de ficheros de documentos .pdf ampliamente utilizado en X Window. Ha aparecido un problema con xpdf que permitiría a un fichero PDF hostil ejecutar código arbitrario. El fallo con xpdf tiene un efecto maremoto, ya que su código ha sido incorporado a otros programas. (CVE-2007-3387)

Debido a los problemas del programa xpdf, los usuarios de la suite de programas y kdgraphics de KOffice de KDE deberán comprobar sus actualizaciones. Los de Gnome deberán comprobarlas para el paquete gpdf.

También deberán comprobar las actualizaciones para los paquetes pdftok.frame-work, tetex-bin, libex-tractor, poppler y pdftohtml. ■

*Referencia Debian: DSA-1347, DSA-1348, DSA-1349, DSA-1350, DSA-1352, DSA-1354, DSA-1355 y DSA-1357*

*Referencia Fedora: FEDORA-2007-1383, FEDORA-2007-1547, FEDORA-2007-1594 y FEDORA-2007-1614*

*Referencia Mandriva: MDKSA-2007:158, MDKSA-2007:160, MDKSA-2007:161, MDKSA-2007:163*

*Referencia Red Hat: RHTSA-2007:0732 y RHTSA-2007:0731-3*

*Referencia SUSE: SUSE-SR:2007:015 y SUSE-SR:2007:016*

*Referencia Ubuntu: USN-496-1 y USN-496-2*

## Firefox, Thunderbird, Seamonkey, IceApe, XULRunner

Firefox, Thunderbird, Seamonkey, IceApe y XULRunner tienen problemas debido a la dependencia del código de Mozilla. Un problema en la ventana "about:blank" podría permitir que un atacante modificara el contenido de un sitio web. (CVE-2007-3844)

El software escapa indebidamente las dobles comillas y espacios en las URLs, lo que podría permitir que un atacante pasara un argumento arbitrario a un programa de ayuda si un usuario es engañado para que abra una página web hostil. (CVE-2007-3845) ■

*Referencia Debian: DSA-1345, DSA-1346*

*Referencia Gentoo: GLSA-200708-09*

*Referencia SUSE: SUSE-SR:2007:049*

*Referencia Ubuntu: USN-493-1, USN-503-1*

## Asterisk

Se han descubierto algunos problemas en Asterisk, un sistema de teléfono de centralita privada que se conecta a la red pública (PBX o private branch exchange)

de código abierto muy popular. Asterisk proporciona funcionalidades de sistemas comerciales en ordenadores personales.

Tres problemas distintos en la sesión del protocolo de iniciación (SIP) podrían conducir a un ataque de denegación de servicio. (CVE-2007-1306, CVE-2007-1561, CVE-2007-2297)

Dos problemas en el driver del canal IAX2 podrían ser explotados por un atacante para llevar a cabo un ataque de denegación de servicio u obtener información del servidor Asterisk. (CVE-2007-2488, CVE-2007-3763)

Un problema IAX2 podría permitir que un atacante ejecutara código arbitrario en una máquina remota. (CVE-2007-3762)

Han aparecido otros dos problemas distintos que podrían permitir situaciones de denegación de servicio. (CVE-2007-2294, CVE-2007-3764) ■

*Referencia Debian: DSA-1358-1*

*Referencia SUSE: SUSE-SR:2007:015*

## Dovecot

Dovecot es un servidor de correo seguro que soporta buzones de correo mbox y maildir. Cuando Dovecot está configurado para usar colas de correo no del sistema de usuario con carpetas comprimidas, el programa permite nombres de buzones de correo en directorios travesados. Un atacante podría leer los contenidos de un fichero de correo .gzip. (CVE-2007-2231) ■

*Referencia Debian: DSA-1359*

*Referencia Ubuntu: USN-487-1*

## VIM

Han aparecido dos errores en VIM, un editor de textos para la línea de comandos. Un problema en la cadena de formato podría llevar a la ejecución de código arbitrario. También, debido a un problema con el cajón de arena, un mecanismo que evita comandos potencialmente perjudiciales de ejecutar, un fichero de texto cuidadosamente construido podría hacer que VIM ejecutara comandos de la shell. (CVE-2007-2953, CVE-2007-2438) ■

*Referencia Debian: DSA-1364*

*Referencia SUSE: SUSE-SR:2007:018*