

INSEGURIDADES

■ Squid

Squid es un proxy cacheador de páginas web. Se ha encontrado un fallo en la manera en la que presenta los mensajes de error. Un atacante podría enviar una petición conteniendo un nombre de host inválido, que resultaría en la presentación de un mensaje de error usado previamente. El Proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE – <http://cve.mitre.org>) ha asignado a este problema el nombre CAN-2005-2479.

Se encontraron dos errores de Denegación de Servicio (el sistema se cuelga) en el modo en el que Squid maneja las peticiones malformadas. Un atacante remoto podría presentar una petición especialmente manipulada que haría que el sistema se colgara. El Proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE – <http://cve.mitre.org>) ha asignado a estos problemas los nombres CAN-2005-2794 y CAN-2005-2796 respectivamente. ■

-Referencia Debian:

DSA-809-2 apache2

-Referencia Mandriva:

MDKSA-2005:162

-Referencia Red Hat: RHSA-2005:766-7

-Referencia Suse: SUSE-SA:2005:053

■ Clam Antivirus

Clam Antivirus es un juego de herramientas anti-virus con licencia GPL diseñado para su integración en servidores de correo para mejorar el escaneado de adjuntos. También ofrece un escáner desde la línea de comando, así como una herramienta para buscar actualizaciones para la base de datos de virus.

Existe una vulnerabilidad de desbordamiento de búfer en *libclamav/upx.c* cuando procesa paquetes ejecutables UPX malformados. *libclamav/fsg.c* también puede caer en un bucle infinito cuando procesa ejecutables empaquetados FSG especialmente manipulados.

Mediante el envío de un fichero especialmente manipulado, un atacante podría ejecutar código arbitrario con los permisos de otro usuario de Clam Antivirus o provocar una Denegación de Servicio (el sistema se cuelga). ■

-Referencia Debian:

DSA-824-1 apache2

-Referencia Gentoo: GLSA 200509-1

-Referencia Mandriva:

MDKSA-2005:166

-Referencia Suse: SUSE-SA:2005:055

■ X.org y XFree86

X.org y XFree86 son implementaciones del Sistema X Window. Ofrecen la funcionalidad de bajo nivel básica para interfaces de usuario gráficas (GUI) sobre las que se apoyan gestores de ventanas tales como GNOME y KDE.

Se encontraron varios errores de desbordamiento de entero en el modo en el que X analiza imágenes pixmap. Es posible que un usuario consiga privilegios elevados cargando una imagen pixmap especialmente manipulada. El Proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE – <http://cve.mitre.org>) ha asignado el nombre CAN-2005-2495 a este problema. ■

-Referencia Debian: DSA-816-1

-Referencia Mandriva:

MDKSA-2005:164

-Referencia Red Hat: RHSA-2005:396-9

-Referencia Slackware:

SSA:2005-269-02

-Referencia Suse: SUSE-SA:2005:056

■ util-linux

util-linux es una juego de útiles programas Linux, incluyendo umount, un programa para desmontar sistemas de ficheros.

Cuando un usuario normal monta un sistema de ficheros, se encuentra sometido a restricciones en el fichero de configuración */etc/fstab*. David Watson descubrió que cuando se desmonta un fichero con la opción *-r*, se activa el bit de sólo

lectura, mientras que otros bits como el *nosuid* o *nodev*, no, incluso si ya lo estuvieron previamente.

Un usuario sin privilegios frente a restricciones *nosuid* o *nodev* puede usar *umount -r* en un sistema de ficheros para desactivar esos bits, permitiendo que las aplicaciones sean ejecutadas *suid*, o interpretar nodos de dispositivos. En el caso de que el usuario puede modificar libremente el contenido del sistema de ficheros, puede darse un escalamiento de privilegios cuando un programa cliente se ejecute con permisos *suid*.

Existen dos soluciones a este tema: el bit *suid* puede cambiarse desde la utilidad *umount*, o pueden restringirse los privilegios de montaje y desmontaje de los usuarios desde */etc/fstab*. Todos los usuarios de util-linux deberían actualizarse a la última versión. ■

-Referencia Debian: DSA-823-1

-Referencia Gentoo: GLSA 200509-15

-Referencia Mandriva:

MDKSA-2005:167

-Referencia Slackware:

SSA:2005-255-02

■ CUPS

El Sistema de Impresión Común UNIX (CUPS) ofrece una capa de impresión portable para sistemas operativos Unix(R).

Se encontró un error en la manera en la que CUPS procesa las peticiones HTTP malformadas. Es posible que un usuario remoto capaz de conectarse a demonios CUPS emita una petición HTTP GET malformada que haga que CUPS caiga en bucle infinito. El Proyecto de Vulnerabilidades y Exposiciones Comunes (Common Vulnerabilities and Exposures o CVE – <http://cve.mitre.org>) ha asignado a este problema el nombre CAN-2005-2874. ■

-Referencia Mandriva:

MDKSA-2005:138-1

-Referencia Red Hat:

RHSA-2005:772-8