PRESIDENCIA DEL CONSEJO DE MINISTROS

Oficina Nacional de GOBIERNO ELECTRÓNICO e INFORMÁTICA

BOLETIN DE SEGURIDAD DE LA INFORMACIÓN

Centro de Consulta e Investigación sobre Seguridad de la Información

Edición Nº 77/ 30 de Diciembre de 2008

Visite el Portal del Estado Peruano: www.peru.gob.pe

CONTENIDO

FUENTES

- Hispasec
- SunSolve
- Info Security
- Adobe.com
- lists.debian.org
- Red Hat

ACTUALIZACIÓN DE SNMP MANAGEMENT AGENT PARA SUN SOLARIS 8, 9 Y 10

Sun ha publicado una actualización para SNMP Management Agent, para evitar una vulnerabilidad que podría permitir a un atacante local obtener privilegios de administrador.

La vulnerabilidad reside en un error en la gestión de archivos temporales, que puede ser aprovechada para sobreescribir archivos arbitrarios y obtener privilegios de root.

Se ven afectadas las versiones de Sun SNMP Management Agent "SUNWmasf" 1.4u2 a 1.5.4 (para Solaris 8, 9 y 10 en plataforma SPARC). Sin embargo, el demonio System Management Agent (SMA) SNMP (snmpd(1M)) incluido en Solaris 10 no se ve afectado.

Sun ha publicado la version Sun SNMP Management Agent ("SUNWmasf") 1.5.5 que corrige el problema disponible desde:

http://www.sun.com/download/

MÁS INFORMACIÓN:

- **Insecure Temporary File Usage Vulnerability in Sun SNMP Management Agent**
  http://sunsolve.sun.com/search/document.do?assetkey=1-66-248646-1

ACTUALIZACIÓN DEL KERNEL PARA DEBIAN LINUX 4.X

Debian ha publicado una actualización del kernel que corrige múltiples fallos de seguridad que podrían causar una denegación de servicio o una elevación de privilegios.

Los problemas corregidos son:

- *Denegación de servicio local o escalada de privilegios en rch/i386/kernel/sysenter.c a través de las funciones install_special_mapping, syscall y syscall32_nopage.*
- *Denegación de servicio local a través de los sistemas de archivos ext2 y ext3. Un usuario local con permisos para montar sistemas de archivos podría crear un sistema de archivos especialmente manipulado pudiendo hacer que el kernel envíe mensajes de error de forma indefinida.*
- *Salto de restricciones de seguridad a través de splice() en archivos abiertos con O_APPEND, que podría permitir la escritura en dicho archivo.*
- *Posibles denegaciones de servicio remoto a través del subsistema SCTP (kernel oops y kernel panic).*
- *Denegaciones de servicio local a través del sistema de archivos hfsplus. Un usuario local con permisos para montar sistemas de archivos podría crear un sistema de archivos especialmente manipulado que podría dar lugar a una corrupción de memoria o kernel oops.*

- *Denegación de servicio, a través del subsistema de sockets unix, que podría causar una corrupción de memoria o kernel panic.*
- *Denegación de servicio, a través de la función svc_listen de net/atm/proc.c. Un usuario local podría provocar un bucle infinito mediante dos llamadas a svc_listen hacia el mismo socket y, a continuación, una lectura del archivo /proc/net/atm/*em.*
- *Elevación de privilegios a través de inotify. Un usuario local podría obtener una elevación de privilegios a través de vectores desconocidos relacionados con condiciones de carrera en inotify y umount.*
- *Denegación de servicio a través de la función sendmsg y AF_UNIX. Un usuario local mediante múltiples llamadas a la función sendmsg podría causar una denegación de servicio debido a que AF_UNIX no bloquea estas peticiones durante la recolección de basura y provoca una condición OOM.*

Se recomienda actualizar a través de las herramientas automáticas
apt-get.

MÁS INFORMACIÓN:

o **[DSA 1687-1] New Linux 2.6.18 packages fix several vulnerabilities**
http://lists.debian.org/debian-security-announce/2008/msg00279.html

VULNERABILIDAD CRÍTICA EN ADOBE FLASH PLAYER PARA LINUX

Adobe ha publicado una actualización de Adobe Flash Player para Linux que soluciona una vulnerabilidad crítica que podría permitir a un atacante ejecutar código arbitrario. El reproductor de Flash de Adobe para Windows o Mac OS X no se ve afectados por el problema.

Adobe no ha proporcionado los detalles técnicos del problema. Especifica que al reproducir un fichero SWF especialmente manipulado, un atacante podría "tomar el control del sistema Linux". Traduciendo, es más que probable que la vulnerabilidad permita la ejecución de código, y que si el usuario que se ve afectado tiene todos los privilegios, el atacante podría tomar el control total del sistema.

Se ven afectadas todas las versiones Adobe Flash Player para Linux anteriores a 10.0.12.36 y 9.0.151.0 (ambas incluidas). Se recomienda que actualicen a la versión 10.0.15.3 o 9.0.152.0.

MÁS INFORMACIÓN:

o **Security update available for Linux Flash Player 10.0.12.36 and Linux - Flash Player 9.0.151.0**
http://www.adobe.com/support/security/bulletins/apsb08-24.html

ACTUALIZACIÓN DEL KERNEL PARA RED HAT ENTERPRISE LINUX 5

Red Hat ha publicado una actualización para el kernel de Red Hat Enterprise Linux 5 que soluciona varios problemas de seguridad y corrige además numerosos bugs.

Los principales problemas corregidos son:

- *El driver i915 del kernel no restringe la ioctl DRM_I915_HWS_ADDR al master Direct Rendering Manager (DRM) . Esto podría permitir a un atacante local elevar privilegios. Sólo afecta a Intel G33 y posteriores.*
- *Un problema de falta de comprobación en ficheros abiertos con O_APPEND en la función sys_splice. Esto podría permitir a un atacante local eludir restricciones de agregar a ficheros arbitrarios.*
- *Un problema en la implementación del protocolo Stream Control Transmission Protocol (SCTP). Esto podría llevar a una posible denegación de servicio en un extremo si una de las conexiones no soporta la extensión AUTH.*

Se recomienda actualizar a través de las herramientas automáticas up2date.

MÁS INFORMACIÓN:

o **Important: kernel security and bug fix update**
http://rhn.redhat.com/errata/RHSA-2008-1017.html

CENTRO DE CONSULTA E INVESTIGACION SOBRE SEGURIDAD DE LA INFORMACION
CCISI

EMAIL:
ccisi@pcm.gob.pe

TELEFONO
2744356 – 106