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 68/ 25 de Marzo de 2008

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

CONTENIDO

FUENTES

- o IBM
- o Cisco
- o Red Hat
- o Open Suse
- o Apple
- o Hispasec

VULNERABILIDADES EN EL KERNEL DE IBM AIX 5.X Y 6.X

IBM ha publicado una actualización para el kernel de los sistemas AIX 5.x y 6.x que soluciona múltiples problemas de seguridad que podrían permitir a un atacante ejecutar código arbitrario, provocar una denegación de servicio u obtener información sensible.

Las vulnerabilidades corregidas son:

- Un proceso de 64 bits que sea reiniciado podría llegar a tener acceso de lectura y escritura en ciertas áreas de la memoria del kernel, lo que podría permitir la ejecución de código arbitrario.
- Nodos remotos de un grupo de volúmenes concurrentes podrían dejar de responder después de que un nodo reduzca su tamaño en un sistema de ficheros JFS2 y resida en el grupo de volúmenes. Esto podría resultar en una denegación de servicio.
- El sistema de ficheros proc no aplica los controles de acceso a directorio correctamente cuando los permisos en un directorio son más restrictivos que los permisos en el directorio actual desde donde se ejecuta el comando. Esto puede derivar en una fuga de información.
- Trusted Execution no protege los ficheros cuando las modificaciones se hacen a través de enlaces duros. Afecta sólo a AIX 6.1.
- Algunas llamadas de sistema WPAR específicas podrían provocar un comportamiento inesperado, resultando en una denegación de servicio. Afecta sólo a AIX 6.1.
- Un usuario con privilegios para ejecutar ProbeVue podría leer cualquier dirección de memoria del kernel, provocando una fuga de información. Afecta sólo a AIX 6.1.

MÁS INFORMACIÓN:

- **IBM**
  http://aix.software.ibm.com/aix/efixes/security/kernel_fix.tar
- **AIX kernel multiple security vulnerabilities**
  http://www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd?mode=18&ID=4155

VULNERABILIDADES EN CISCO SECURE ACS PARA WINDOWS

Se han encontrado dos vulnerabilidades en la aplicación User-Changeable Password (UCP) en Cisco Secure Access Control Server (ACS) para Windows :

- La primera vulnerabilidad está causada por varios desbordamientos de búfer en el código CSuserCGI.exe de la aplicación UCP, que podría ser aprovechado por un atacante remoto para ejecutar código arbitrario.
- La segunda es una vulnerabilidad de cross-site scripting en la página web de la aplicación UCP (en el código CsuserCGI.exe), que podría ser aprovechada por un atacante remoto para ejecutar código HTML o JavaScript arbitrario en el contexto de seguridad del navegador de un usuario que visita la web afectada.

MÁS INFORMACIÓN:

- **Cisco Secure Access Control Server for Windows User-Changeable Password Vulnerabilities**
  http://www.cisco.com/warp/public/707/cisco-sa-20080312-ucp.shtml

ACTUALIZACIÓN DEL KERNEL PARA RED HAT ENTERPRISE LINUX 4

El problema está causado por un desbordamiento de búfer en el sistema de archivos virtual CIFS que podría ser aprovechado por un atacante remoto autenticado para ejecutar código arbitrario o causar una denegación de servicio.
Se recomienda actualizar a través de las herramientas automáticas up2date.

MÁS INFORMACIÓN:

- **Moderate: kernel security and bug fix update**
  http://rhn.redhat.com/errata/RHSA-2008-0167.html

ACTUALIZACIÓN PARA PRODUCTOS SUSE LINUX

SuSE ha publicado varias actualizaciones para diferentes paquetes que solucionan diversos problemas de seguridad. Las actualizaciones afectan a OpenSUSE Linux 10.x y SuSE Linux 10.x.

Los paquetes y problemas corregidos son:

- Desbordamientos de memoria intermedia en sarg que podrían permitir a un atacante ejecutar código arbitrario.
- Múltiples problemas de cross site scripting en phpMyAdmin.
- Desbordamientos de memoria intermedia en xine podrían permitir a un atacante ejecutar código arbitrario.
- Desbordamientos de memoria intermedia en libbind podrían permitir a un atacante ejecutar código arbitrario.
- Problemas de aplicación de políticas en dbus-1 podrían permitir a un atacante acceder a información sensible.
- Desbordamientos de memoria intermedia en sensible.silc-toolkit podrían permitir a un atacante ejecutar código arbitrario.
- Denegación de servicio a través de expresiones regulares en boost.

MÁS INFORMACIÓN:

- **[security-announce] SUSE Security Summary Report SUSE-SR:2008:006**
  http://lists.opensuse.org/opensuse-security-announce/2008-03/msg00004.html

VULNERABILIDAD EN APPLE MAC OS X

Apple ha lanzado recientemente una nueva actualización de seguridad para su sistema operativo Mac OS X que solventa más de 90 vulnerabilidades que podrían ser aprovechadas por un atacante local o remoto para saltarse restricciones de seguridad, perpetrar ataques de cross-site scripting, acceder a información sensible, escalar privilegios, provocar denegaciones de servicio o incluso ejecutar código arbitrario en un sistema vulnerable.

A continuación se exponen con brevedad algunas de las vulnerabilidades solucionadas:

- Errores de límite en AFP client que podían ser aprovechados para ejecutar código arbitrario.

- Múltiples vulnerabilidades en AppKit.
- Una vulnerabilidad en Application Firewall aprovechada para saltar restricciones de seguridad.
- Una vulnerabilidad en CFNetwork aprovechada para falsificar websites seguros.
- Múltiples vulnerabilidades en ClamAV.
- Una vulnerabilidad en CoreFoundation que podría ser aprovechada por un
- atacante local para ejecutar código arbitrario.
- Una vulnerabilidad en CoreServices y que podría ser explotada por un atacante remoto para saltar restricciones de seguridad.
- Una vulnerabilidad en file que podría ser explotada por un atacante remoto para provocar una denegación de servicio.
- Una vulnerabilidad en Help Viewer que podría ser explotada por un atacante remoto para ejecutar código Applescript arbitrario.
- Múltiples vulnerabilidades en PHP.

ACTUALIZACIONES:

- **Security Update 2008-002 v1.0 (PPC):**
  http://www.apple.com/support/downloads/securityupdate2008002v10ppc.html
- **Security Update 2008-002 v1.0 (Universal):**
  http://www.apple.com/support/downloads/securityupdate2008002v10universal.html
- **Security Update 2008-002 v1.0 (Leopard):**
  http://www.apple.com/support/downloads/securityupdate2008002v10leopard.html
- **Security Update 2008-002 v1.0 Server (Leopard):**
  http://www.apple.com/support/downloads/securityupdate2008002v10serverleopard.html
- **Security Update 2008-002 v1.0 Server (PPC):**
  http://www.apple.com/support/downloads/securityupdate2008002v10serverppc.html
- **Security Update 2008-002 v1.0 Server (Universal):**
  http://www.apple.com/support/downloads/securityupdate2008002v10serveruniversal.html

CONGRESOS Y SEMINARIOS DEL 2008
Junio 18 al 20 de 2008: **VIII Jornada Nacional de Seguridad Informática ACIS 2008 (Bogotá - Colombia)** http://www.acis.org.co/index.php?id=1066
Junio 23 al 25 de 2008: **The 5th International Conference on Autonomic and Trusted Computing (Oslo - Noruega)** http://www.ux.uis.no/atc08/
Junio 25 al 27 de 2008: **Sexto Congreso Collaborative Electronic Communications and eCommerce Technology and Research CollECTeR Iberoamérica 2008 (Madrid - España)** http://www.collecter.euitt.upm.es/
Julio 9 al 11 de 2008: **XIV Jornadas de Enseñanza Universitaria de la Informática (Granada - España)** http://jenui2008.ugr.es/
Septiembre 2 al 5 de 2008: **X Reunión Española de Criptología y Seguridad de la Información RECSI 2008 (Salamanca - España)** http://www.usal.es/~xrecsi/
Septiembre 10 al 12 de 2008: **EATIS 2008 Euro American Conference on Telematics and Information Systems (Aracajú - Brasil)** http://eatis.org/eatis2008/

CUALQUIER CONSULTA ENVIAR UN CORREO AL CENTRO DE CONSULTA E INVESTIGACION SOBRE SEGURIDAD DE LA INFORMACION CCISI

EMAIL:
ccisi@pcm.gob.pe

TELEFONO
2744356 – 106