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 70/ 26 de Mayo de 2008

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

CONTENIDO

- ACTUALIZACIÓN DEL KERNEL PARA PRODUCTOS NOVELL SUSE LINUX
- VULNERABILIDAD EN ADOBE READER Y ACROBAT
- VULNERABILIDADES EN CISCO UNIFIED COMMUNICATIONS MANAGER
- CONGRESOS Y SEMINARIOS DE SEGURIDAD EN EL 2008

FUENTES

- Hispasec
- Novell
- Adobe
- Info Security
- VSAntivirus

ACTUALIZACIÓN DEL KERNEL PARA PRODUCTOS NOVELL SUSE LINUX

Novell ha publicado una actualización de kernel de SuSE Linux que corrige diversas vulnerabilidades.

1. Se ha corregido un fallo no especificado que permitía a un atacante local efectuar una denegación de servicio a través de vectores no especificados.
2. Condición de carrera en dnotify que podría permitir un atacante local causar una denegación de servicio.
3. Un atacante remoto podría causar una denegación de servicio en la pila IPSec/IPv6 por medio de paquetes ESP especialmente manipulados.
4. Se ha corregido un fallo que borraba el flag de dirección antes de llamar a manejadores de señal, que podría permitir a un atacante remoto ejecutar código arbitrario en algunos programas no especificados bajo ciertas condiciones.

Según versión y plataforma las actualizaciones están disponibles en:

- *Para SuSE Linux Enterprise Server 9 (PowerPC):*
  http://download.novell.com/Download?buildid=eQZcmmRQ7oQ~
- *Para Novell Linux POS 9 (x86):*
  http://download.novell.com/Download?buildid=BKgGfKKLd3E~
- *SuSE Linux Enterprise Server 9 (x86):*
  http://download.novell.com/Download?buildid=27kCZ1qWwWo~
- *SuSE Linux Enterprise Server 9 (x86-64):*
  http://download.novell.com/Download?buildid=XxaBNf2VYTU~
- *Novell Linux Desktop 9 (AMD x86-64):*
  http://download.novell.com/Download?buildid=4Ye2fNZ9fYY~

MÁS INFORMACIÓN:

- **Linux kernel 20080610**
  http://support.novell.com/docs/Readmes/InfoDocument/patchbuilder/readme_5028579.html

VULNERABILIDAD EN ADOBE READER Y ACROBAT

Se ha encontrado una vulnerabilidad en Adobe Reader y Acrobat que podría permitir a un atacante ejecutar código arbitrario.

El fallo se debe a un error de validación de entrada en el método JavaScript que podría permitir la ejecución de código si se abre con el programa vulnerable un archivo especialmente manipulado.

Para Reader se recomienda instalar el Adobe Reader 8.1.2 Security Update 1 patch, disponible:

- *Para Windows:*
  http://www.adobe.com/support/downloads/detail.jsp?ftpID=3967
- *Para Macintosh:*
  http://www.adobe.com/support/downloads/detail.jsp?ftpID=3966

Para Acrobat se recomienda instalar el Adobe Acrobat 8.1.2 Security Update 1 patch, disponible:

- *Para Windows:*
  http://www.adobe.com/support/downloads/detail.jsp?ftpID=3976
- *Para Macintosh:*
  http://www.adobe.com/support/downloads/detail.jsp?ftpID=3977

Para Adobe Reader 7.0 y 7.0.9 se recomienda actualizar a 7.1.0 desde:

- http://www.*adobe*.com/go/getreader.

MÁS INFORMACIÓN:

- **Security Update available for Adobe Reader and Acrobat 8.1.2**
  http://www.adobe.com/support/security/bulletins/apsb08-15.html
- **Adobe Reader and Acrobat 8.1.2 Security Update**
  http://isc.sans.org/diary.php?storyid=4616

VULNERABILIDADES EN CISCO UNIFIED COMMUNICATIONS MANAGER

Se han encontrado dos vulnerabilidades en Cisco Unified Communications Manager (CUCM) que podrían ser aprovechadas por un atacante remoto para causar una denegación de servicio o para saltarse restricciones de seguridad.

- La primera vulnerabilidad está causada por un fallo en el servicio Computer Telephony Integration (CTI) de las versiones 5.x y 6.x de CUCM al manejar entradas mal formadas, lo que podría causar una denegación de servicio.

- La segunda vulnerabilidad está causada por un fallo en el servicio Real-Time Information Server (RIS) Data Collector de las versiones 4.x, 5.x y 6.x de CUCM que podría permitir un salto de restricciones de seguridad y la revelación de información sensible de clusters CUCM. Conectándose directamente al puerto de escucha del proceso RIS Data Collector (TCP 2556) sería posible saltarse la autenticación y conseguir acceso de lectura a información sobre un cluster CUCM. Esta información podría incluir estadísticas, nombres de usuario y teléfonos IP configurados, pero no incluiría contraseñas u otra información sensible acerca de la configuración de CUCM.

MÁS INFORMACIÓN:

- **Cisco Security Advisory: Cisco Unified Communications Manager Denial of Service and Authentication Bypass Vulnerabilities**
  http://www.cisco.com/warp/public/707/cisco-sa-20080625-cucm.shtml

CONGRESOS Y SEMINARIOS DEL 2008
Mayo 27 al 29 de 2008 **IV Congreso Internacional de Seguridad Electronica (Brasil)** http://www.abese.org.br/cis2008/
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/

CENTRO DE CONSULTA E INVESTIGACION SOBRE SEGURIDAD DE LA INFORMACION CCISI

EMAIL:
ccisi@pcm.gob.pe

TELEFONO
2744356 – 106