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 67/ 22 de Febrero de 2008

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

CONTENIDO

FUENTES

- o Securityfocus
- o IBM
- o Opera
- o Apple
- o Hispasec

VULNERABILIDADES EN IBM DB2 9.X

Se han encontrado varias vulnerabilidades en IBM DB2 9.x, algunas de impacto desconocido y otras que podrían ser aprovechadas por un atacante local o remoto para causar una denegación de servicio.

Los problemas anunciados por IBM son, entre otros:

- Se ha encontrado un error durante el procesado de CONNECT/ATTACH que podría ser aprovechado para causar una denegación de servicio.
- Hay unos errores no especificados en SYSPROC.ADMIN_SP_C, SYSPROC.NNSTAT y Rutinas de administración de ficheros JAR. No se ha suministrado mayor información.

RECOMENDACIÓN:

Se recomienda aplicar el fixpack 4a, disponible desde:
http://www-1.ibm.com/support/docview.wss?rs=71&uid=swg21255572

MÁS INFORMACIÓN:

- **DB2 Version 9.1 for Linux, UNIX and Windows APARs by fix pack**
  http://www-1.ibm.com/support/docview.wss?rs=71&uid=swg21255607

VULNERABILIDAD EN IBM LOTUS NOTES 6.X Y 7.X

La vulnerabilidad está causada por un error en el plugin de Java al procesar código JavaScript especialmente manipulado. Esto podría ser aprovechado por un atacante remoto para comprometer un sistema vulnerable si un usuario abre un email especialmente manipulado que contenga un applet de Java malicioso.

La vulnerabilidad sólo afecta si la opción "Enable Java access from JavaScript" está activada en las preferencias de usuario.

Para Lotus Notes 6.x y 7.x se recomienda actualizar a IBM Lotus Notes versión 7.0.2, disponible desde:

http://www.ibm.com/software/lotus/support/upgradecentral/index.html

MÁS INFORMACIÓN:

- **IBM Lotus Notes Java Plugin Sandbox Security Bypass Vulnerability**
  http://www.frsirt.com/english/advisories/2008/0599/solution

VULNERABILIDADES DE OPERA 9.26 CORREGIDAS

Se han encontrado múltiples vulnerabilidades en Opera:

- La primera vulnerabilidad está causada por un error en el manejo de valores de atributos DOM (Document Object Model) cuando se importa XML a un documento. Se podría dar la circunstancia de que los valores se saltaran los filtros de limpieza, lo que podría ser explotado por un atacante remoto para perpetrar ataques de cross-site scripting si los valores son usados como contenido del documento.

- Otra vulnerabilidad está causada por un fallo de diseño al manejar las entradas de archivo en campos de formularios, y podría ser aprovechada por un atacante remoto para engañar a un usuario para que subiera archivos arbitrarios a la red, revelando así información sensible.

- La última vulnerabilidad está causada por un fallo en el manejo de comentarios "a medida" (custom comments) contenidos en las propiedades de una imagen. Cuando se muestran las propiedades de la imagen, Opera podría tratar por error los comentarios como un script, lo que podría ser aprovechado por un atacante remoto para ejecutar código JavaScript arbitrario en un contexto de seguridad incorrecto cuando se muestran los comentarios de una imagen especialmente manipulada.

Las vulnerabilidades están confirmadas para las versiones anteriores a la 9.26.

RECOMENDACIONES:

Se recomienda actualizar a la versión 9.26 de Opera, disponible desde:
http://www.opera.com/download/

MAS INFORMACIÓN:

- **Advisory: Representation of DOM attribute values could allow cross-site scripting**
  http://www.opera.com/support/search/view/880/

- **Advisory: Simulated text inputs can trick users into uploading arbitrary files**
  http://www.opera.com/support/search/view/877/

- **Advisory: Image properties can be used to execute scripts**
  http://www.opera.com/support/search/view/879/

- **Serious Browser Bugs Spoil Opera Tune**
  http://www.eweek.com/c/a/Security/Serious-Browser-Bugs-Spoil-Opera-Tune/

ACTUALIZACIÓN DE SEGURIDAD PARA APPLE MAC OS X

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

Las actualizaciones a la versión 10.5.2 pueden ser instaladas a través de la funcionalidad de actualización (Software Update) de Mac OS X o, según versión y plataforma, descargándolas directamente desde:

- **Security Update 2008-001 (PPC):**
  http://www.apple.com/support/downloads/securityupdate2008001ppc.html

- **Security Update 2008-001 (Universal):**
  http://www.apple.com/support/downloads/securityupdate2008001universal.html

- **Mac OS X 10.5.2 Combo Update:**
  http://www.apple.com/support/downloads/macosx1052comboupdate.html

- **Mac OS X Server 10.5.2 Combo Update:**
  http://www.apple.com/support/downloads/macosxserver1052comboupdate.html

MÁS INFORMACIÓN:

- **About the security content of Mac OS X 10.5.2 and Security Update 2008-001**
  http://docs.info.apple.com/article.html?artnum=307430

CONGRESOS Y SEMINARIOS DEL 2008
Marzo 13 al 15 de 2008: **4th Workshop on Coding and Systems (Alicante y Elche - España)** http://www.dccia.ua.es/wcs2008
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