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 76/ 27 de Noviembre de 2008

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

CONTENIDO

- DOS VULNERABILIDADES EN 2.X DE OPENOFFICE
- ACTUALIZACIÓN DEL KERNEL PARA SUN SOLARIS 8, 9, 10 Y OPENSOLARIS
- ERNST & YOUNG PUBLICA LOS RESULTADOS DE LA XI ENCUESTA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN

FUENTES

- Hispasec
- OpenOffice
- SunSolve
- Info Security

DOS VULNERABILIDADES EN 2.X DE OPENOFFICE

OpenOffice.org ha publicado una actualización para la rama 2.x de OpenOffice. Soluciona dos problemas de seguridad que podrían permitir a un atacante ejecutar código si se procesan documentos especialmente manipulados con una versión vulnerable.

* Uno de los fallos se trata de un desbordamiento de memoria intermedia basado en heap en el intérprete de ficheros EMF.

* El segundo fallo se debe a un desbordamiento de enteros a la hora de procesar registros META_ESCAPE en ficheros WMF.

Ambos fallos podrían permitir la ejecución de código arbitrario con los permisos del usuario bajo el que se usara la aplicación.

La reciente versión 3.0 de OpenOffice no se ve afectada.

No se han dado detalles técnicos ni parece existir exploit público. Se recomienda actualizar a la versión OpenOffice 2.4.2. Todas las anteriores son vulnerables.

MÁS INFORMACIÓN:

- **Manipulated EMF files can lead to heap overflows and arbitrary code execution**
  http://www.openoffice.org/security/cves/CVE-2008-2237.html
- **Manipulated WMF files can lead to heap overflows and arbitrary code execution**
  http://www.openoffice.org/security/cves/CVE-2008-2238.html

ACTUALIZACIÓN DEL KERNEL PARA SUN SOLARIS 8, 9, 10 Y OPENSOLARIS

Sun ha dado a conocer un fallo en el kernel de Solaris que permitiría a usuarios locales eludir restricciones de seguridad.

La vulnerabilidad reside en un error en el kernel relacionado con las llamadas al sistema. Un atacante podría saltarse el modo multi-nivel en la política de seguridad de Solaris Trusted Extensions o en la política
de aislamiento por zonas, chroot.

Sun ha publicado los siguientes parches disponibles, según versión y plataforma:

Para la plataforma SPARC:

- Solaris 8 aplicar actualización 117350-56 o superior, desde:
  http://sunsolve.sun.com/search/document.do?assetkey=1-21-117350-56-1

- Solaris 9 aplicar actualización 122300-30, desde: http://sunsolve.sun.com/search/document.do?assetkey=1-21-122300-30-1
- Solaris 10 aplicar actualización 137111-05, desde: http://sunsolve.sun.com/search/document.do?assetkey=urn:cds:docid:1-21-137111-05-1

Para plataforma x86:

- Solaris 8 aplicar actualización 117351-56 desde: http://sunsolve.sun.com/search/document.do?assetkey=urn:cds:docid:1-21-117351-56-1

- Solaris 9 aplicar actualización 122301-30, desde: http://sunsolve.sun.com/search/document.do?assetkey=urn:cds:docid:1-21-122301-30-1

- Solaris 10 aplicar actualización 137112-05, desde: http://sunsolve.sun.com/search/document.do?assetkey=urn:cds:docid:1-21-137112-05-1

MÁS INFORMACIÓN:

o **Covert Channel Security Vulnerability in the Solaris Kernel**
http://sunsolve.sun.com/search/document.do?assetkey=1-66-240706-1

ERNST & YOUNG PUBLICA LOS RESULTADOS DE LA XI ENCUESTA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN

La consultora Ernst & Young ha publicado los resultados de la Encuesta Global de Seguridad de la Información (Global Information Security Survey) en su undécima edición, en la que se ofrece una mirada al actual estado de la seguridad de la información y ofrece recomendaciones para la mejora de cara al futuro.

La encuesta se realizó entre junio y agosto de este año, entre 1.400 organizaciones de más de 50 países de todo el mundo. Entre los resultados a destacar cabe mencionar la cada vez mayor preocupación por el impacto que puede tener un incidente de seguridad en la reputación e imagen de marca. Un 85% de los encuestados reseñaron los daños a la reputación y la marca como la consecuencia más importante ante un ataque, frente al 72% que destacó la pérdida de ingresos. Otras consecuencias preocupan aun menos, como las sanciones (68%) o acciones legales (un 65%).

Otro dato a reseñar, es que a pesar de la crisis las empresas parecen conscientes de la importancia de la seguridad de la información y tan solo un 5% de los encuestados dicen que reducirán su presupuesto para esta materia en el año que viene. Incluso, la mitad afirman que aumentarán su gasto en seguridad informática (mientras que un 45% dicen que la mantendrán). Ernst & Young concluye que las organizaciones reconocen que efectuar recortes en materia de seguridad podría tener un efecto contrario, además de que una gran mayoría considera que las amenazas y los ataques aumentarán durante la época de crisis.

El estudio se compone de diez puntos o aspectos sobre los que desglosa la información:

1. *La protección de la reputación y la marca se ha convertido en un importante motor para la seguridad de la información.*
2. *A pesar de las presiones económicas, las organizaciones siguen invirtiendo en seguridad de la información.*
3. *Los estándares internacionales de seguridad de la información están adquiriendo una mayor aceptación y aprobación.*
4. *Muchas organizaciones siguen luchando para lograr una visión estratégica de la seguridad de la información.*
5. *Ahora la privacidad es una prioridad, pero las acciones se quedan cortas.*
6. *Las personas siguen siendo el eslabón más débil en la seguridad de la información.*
7. *Los riesgos del crecimiento de subcontratas no se están corrigiendo.*
8. *La continuidad del negocio sigue dependiendo de tecnología de la información.*
9. *La mayoría de las organizaciones no están dispuestas a externalizar actividades claves de seguridad de la información.*
10. *Pocas empresas cubren los riesgos de seguridad de la información con seguros.*

MÁS INFORMACIÓN:

o **El informe puede descargarse desde:**
http://www.ey.com/Global/assets.nsf/International/TSRS_Global_Information_Security_Survey_2008/$file/TSRS_Global_Information_Security_Survey_2008.pdf

CENTRO DE CONSULTA E INVESTIGACION SOBRE SEGURIDAD DE LA INFORMACION
CCISI

EMAIL:
ccisi@pcm.gob.pe

TELEFONO
2744356 – 106