

CONTENIDO

- ▶ ACTUALIZACION PARA SUN SOLARIS 8, 9 Y 10
- ▶ ACTUALIZACIÓN DEL KERNEL PARA RED HAT ENTERPRISE LINUX 4.X
- ▶ VULNERABILIDADES DE FIREFOX 2.0.0.15
- ▶ ORACLE PUBLICARÁ PARCHES PARA 45 PROBLEMAS DE SEGURIDAD
- ▶ VULNERABILIDAD EN REALPLAYER
- ▶ CONGRESOS Y SEMINARIOS DE SEGURIDAD EN EL 2008

ACTUALIZACION PARA SUN SOLARIS 8, 9 Y 10

Sun Solaris ha publicado una actualización para Solaris 8, 9 y 10 que solventa una vulnerabilidad en picld que podría ser aprovechada por un atacante local para causar una denegación de servicio.

La vulnerabilidad está causada por un error en el picld que podría ser aprovechado por un atacante local para deshabilitar sistemas de monitorización y provocar que las utilidades prtdiag, prtpicl o prtfru dejen de funcionar de forma adecuada.

Según versión y plataforma, se recomienda instalar los siguientes parches:

Para la plataforma SPARC:

- Solaris 8 instalar el parche 112169-07 o superior.
- Solaris 9 instalar el parche 137400-01 o superior.
- Solaris 10 instalar el parche 138068-01 o superior.

Para la plataforma x86:

- Solaris 9 instalar el parche 137401-01 o superior.
- Solaris 10 instalar el parche 138069-01 o superior.

MÁS INFORMACIÓN:

- **A Security Vulnerability in picld(1M) May Allow a Denial of Service to System Monitoring and System Services**
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-239728-1>

ACTUALIZACIÓN DEL KERNEL PARA RED HAT ENTERPRISE LINUX 4.X

Red Hat ha publicado una actualización del kernel de Red Hat Desktop, Enterprise Linux AS, ES y WS en su versión 4 que corrige varios fallos de seguridad que podrían permitir a un atacante local causar una denegación de servicio o acceder a información sensible.

- Se ha encontrado un fallo en las rutinas de copia de memoria en el kernel de Linux.
- Se ha descubierto una condición de carrera en ptrace que podría ser aprovechada por un atacante local para causar una denegación de servicio en el sistema (kernel hang).
- Existe un fallo en la emulación de los kernel de 32 y 64 bits que podría ser aprovechado por un atacante para causar una fuga de datos por medio de un binario especialmente manipulado.
- Se ha descubierto que el kernel de Linux manejaba las operaciones de cadenas de una forma opuesta a la de GNU Compiler Collection (GCC). Esto podría ser aprovechado por un atacante local sin privilegios para causar la corrupción de la memoria.

La actualización también solventa otro fallo de menor importancia.

Se recomienda actualizar a través de las herramientas automáticas up2date.

MÁS INFORMACIÓN:

- **kernel security and bug fix update**
<https://rhn.redhat.com/errata/RHSA-2008-0508.html>

FUENTES

- Hispasec
- Info Security
- VSAntivirus
- Sun Solaris
- Red Hat
- Oracle

VULNERABILIDADES DE FIREFOX 2.0.0.15

Las versiones de Firefox 2.0.0.14 y anteriores, contienen una vulnerabilidad que puede permitir a un atacante la ejecución de código. Los usuarios que utilicen las versiones 2.0 de este navegador, deberán actualizarse a la brevedad posible a la versión 2.0.0.15, si no lo han hecho de forma automática.

El problema es un desbordamiento de búfer, y además de Firefox son afectados SeaMonkey y Epiphany, ya que utilizan el mismo componente afectado. Un ataque exitoso puede llegar a comprometer los sistemas donde estos programas se estén ejecutando. Esta vulnerabilidad no afecta a Firefox 3.

La solución es actualizarse a la versión 2.0.0.15. Firefox 2.0.0.15 está disponible para descarga manual, o a través de la actualización automática.

* Descarga de Firefox 2.0.0.15 en español:
<http://releases.mozilla.org/pub/mozilla.org/firefox/releases/2.0.0.15/win32/es-ES/>

MÁS INFORMACIÓN:

- **Known Vulnerabilities in Mozilla Products**
<http://www.mozilla.org/projects/security/known-vulnerabilities.html>
- **Mozilla.org Security Center**
<http://www.mozilla.org/security/>
- **VSantivirus**
<http://www.vsantivirus.com/firefox-2-0-0-15.htm>

ORACLE PUBLICARÁ PARCHES PARA 45 PROBLEMAS DE SEGURIDAD

Para la próxima CPU (Critical Patch Update) de Oracle, se solucionarán 45 problemas de seguridad en total. 11 de estos parches estarán destinados a corregir fallos en Oracle Database, producto "estrella" de la compañía. 9 para Oracle Application Server, 6 para Oracle E-Business Suite, 2 para Oracle Enterprise Manager, 7 para productos Oracle PeopleSoft Enterprise, 7 para Oracle WebLogic Server y 3 para Oracle TimesTen In-Memory Database.

De estos fallos mencionados, al parecer ninguno de los 11 para la base de datos son especialmente graves, pues no necesitarían autenticación para ser aprovechados de forma remota.

Oracle acumula este año 112 problemas de seguridad (a la espera del grupo de parches de octubre), lo que supone una considerable mejora con respecto a años anteriores. En 2007 publicó más de 180 parches. En 2006, batió todas las marcas con casi 300 problemas de seguridad solucionados sólo ese año.

Esta será la primera vez que el grupo de parches de Oracle incluya actualizaciones para WebLogic Server, producto de BEA Systems que fue adquirido por Oracle en enero de este

mismo año. También para Hyperion y TimesTen Database, tecnología también absorbida hace tiempo por el gigante de las bases de datos.

MÁS INFORMACIÓN:

- **Oracle Critical Patch Update Pre-Release Announcement - July 2008**
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html>

VULNERABILIDAD EN REALPLAYER

RealNetworks ha publicado recientemente una actualización de seguridad para su producto más conocido, RealPlayer, que corrige un total de cuatro fallos que podrían ser aprovechados por un atacante remoto para acceder a información sensible, causar una denegación de servicio o ejecutar código arbitrario en un sistema vulnerable.

RealPlayer es un reproductor multimedia disponible para distintas plataformas y que acepta archivos de audio y vídeo en un gran número de formatos. Las vulnerabilidades corregidas, tres de ellas calificadas como críticas.

MÁS INFORMACIÓN:

- **RealNetworks, Inc. Releases Update to Address Security Vulnerabilities.**
http://www.service.real.com/realplayer/security/07252008_player/en/
- **RealNetworks RealPlayer rmoc3260 ActiveX Control Memory Corruption Vulnerability**
<http://www.zerodayinitiative.com/advisories/ZDI-08-047/>
- **Hispasec**
www.hispasec.com

CONGRESOS Y SEMINARIOS DEL 2008
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