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 73/ 27 de Agosto de 2008

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

CONTENIDO

- ACTUALIZACION PARA SUN SOLARIS 8, 9 Y 10
- VULNERABILIDADES A TRAVÉS DE RDESKTOP EN OPENSOLARIS
- LA VERSIÓN 9.52 DE OPERA CORRIGE HASTA SIETE VULNERABILIDADES
- CONGRESOS Y SEMINARIOS DE SEGURIDAD EN EL 2008

FUENTES

- Hispasec
- Sun
- Opera
- Info Security

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

VULNERABILIDADES A TRAVÉS DE RDESKTOP EN OPENSOLARIS

Sun ha publicado una actualización que corrige tres vulnerabilidades que podrían permitir a un atacante remoto causar una denegación de servicio o ejecutar código arbitrario.

- La primera vulnerabilidad está causada por un desbordamiento de enteros en la función iso_recv_msg (en iso.c).
- La segunda vulnerabilidad está causada por un desbordamiento de búfer en la función process_redirect_pdu (en rdp.c).
- La tercera vulnerabilidad está causada por un entero sin signo en la función xrealloc (en rdesktop.c).

Las vulnerabilidades afectan a sistemas X86 y SPARC hasta la compilación 85.

MÁS INFORMACIÓN:

- **Multiple Security Vulnerabilities in rdesktop may lead to Execution of Arbitrary Code or Denial of Service (DOS)**
  http://sunsolve.sun.com/search/document.do?assetkey=1-66-240708-1

LA VERSIÓN 9.52 DE OPERA CORRIGE HASTA SIETE VULNERABILIDADES

Opera, además de ser un navegador web, contiene cliente de correo electrónico con gestor de contactos, cliente de IRC, lector de noticias RSS y gestor para la descarga de archivos torrent.

Se ha lanzado la versión 9.52 del navegador Opera, que corrige un total de siete vulnerabilidades, una de ellas de nivel crítico, que podrían ser aprovechadas por un atacante remoto para perpetrar ataques de falsificación y cross-site scripting, saltarse restricciones de seguridad, revelar información sensible, causar una denegación de servicio o ejecutar código arbitrario en un sistema vulnerable.

De las siete vulnerabilidades corregidas recientemente, la primera está catalogada como extremadamente severa por el equipo de Opera, puesto que permitiría la ejecución remota de código. A continuación se explican con los problemas anteriores:

- Se ha subsanado un fallo de seguridad provocado por un error no especificado en Opera al funcionar como un manejador para ciertos protocolos.
- Se ha corregido una vulnerabilidad que consiste en un error en la manera en que Opera comprueba qué marcos pueden ser modificados en una página web.
- Se ha corregido un fallo no especificado que podría permitir que un atacante remoto perpetrase ataques de tipo cross-site scripting, pudiendo ser explotado para ejecutar código JavaScript o HTML en el contexto de de la sesión del navegador de un usuario que visita un sitio web afectado.
- Se ha solventado una vulnerabilidad que consiste en un error al procesar atajos de teclado personalizados y comandos de menú utilizados para llamar a aplicaciones externas.
- Se ha corregido otro problema causado por un error al indicar en Opera información sobre la seguridad de una pagina web.
- Se ha solventado un posible salto de restricciones de seguridad que podría permitir que un atacante, a través de un script, comprobase la existencia de determinados archivos en un sistema local, por medio de intentos de suscripción a los mismos a través de una página web.
- El último fallo está causado por un error al procesar nuevas peticiones de suscripciones a fuentes (feeds) a través del botón de suscripción.

Las vulnerabilidades están confirmadas para todas las versiones de Opera, desde la 5.x hasta la 9.x.

Se recomienda actualizar a la versión 9.52 del navegador Opera, disponible para su descarga desde:

http://www.opera.com/download/

MÁS INFORMACIÓN:

- **Opera 9.52 for Windows Changelog**
  http://www.opera.com/docs/changelogs/windows/952/

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