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 74/ 30 de Septiembre de 2008

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

CONTENIDO

FUENTES

- Hispasec
- Sun
- Opera
- Info Security

VULNERABILIDADES EN XSUN Y XORG DE SUN SOLARIS 8, 9 Y 10

Sun ha reconocido que Xsun y Xorg contiene múltiples fallos de seguridad que podrían permitir a un atacante local efectuar una denegación de servicio y potencialmente ejecutar código arbitrario.

Los problemas corregidos son:

- Un fallo en la validación de los parámetros de las funciones "SProcSecurityGenerateAuthorization" y "SprocRecordCreateContext".
- Un desbordamiento de entero en la validación de los parámetros de la función "ShmPutImage" (extensión MIT-SHM).
- Un desbordamiento de entero en la función "Allocateglyph" (extensión Render) cuando reserva memoria para el tamaño de un glifo.
- Un desbordamiento de entero en la función "ProcRenderCreateCursor".
- Fallos de desbordamiento de enteros en las funciones "SProcRenderCreateLinearGradient", "SprocRenderCreateRadialGradient" y "SprocRenderCreateConicalGradient".

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

Plataforma SPARC:

Solaris 8 aplicar actualización 119067-10 o superior (para Xsun):
http://sunsolve.sun.com/pdownload.do?target=119067-10&method=h

Solaris 9 aplicar actualización 112785-64 o superior (para Xsun):
http://sunsolve.sun.com/pdownload.do?target=112785-64&method=h

Solaris 10 aplicar actualizaciónes 119059-44 o superior y 125719-12 o superior:
http://sunsolve.sun.com/pdownload.do?target=119059-44&method=h
http://sunsolve.sun.com/pdownload.do?target=125719-12&method=h

Plataforma X86:

Solaris 8 aplicar actualización 119068-10 o superior (para Xsun)
http://sunsolve.sun.com/pdownload.do?target=119068-10&method=h

Solaris 9 aplicar actualización 112786-53 o superior (para Xsun)
http://sunsolve.sun.com/pdownload.do?target=112786-53&method=h

Solaris 9 (with JDS release 2) aplicar actualización 118908-06 o superior (para Xog)
http://sunsolve.sun.com/pdownload.do?target=118908-06&method=h

Solaris 10 aplicar actualizaciones 119060-43 o superior y 125720-23 o superior
http://sunsolve.sun.com/pdownload.do?target=119060-43&method=h
http://sunsolve.sun.com/pdownload.do?target=125720-23&method=h

MÁS INFORMACIÓN:

- **Multiple Security Vulnerabilities in the Solaris X Server Extensions may lead to a Denial of Service (DoS) condition or allow Execution of Arbitrary Code**
  http://sunsolve.sun.com/search/document.do?assetkey=1-66-238686-1

VULNERABILIDAD EN MÚLTIPLES PAQUETES DE SUSE LINUX

SuSE Linux ha publicado un resumen de las actualizaciones se han puesto a disposición de los usuarios:

- Actualización de seguridad de ClamAv que solventa numerosa vulnerabilidades.
- Posible ejecución local de código a través de archivos python al ser editados con emacs.
- Denegación de servicio o ejecución remota de código a través de múltiples desbordamientos de búfer en php5.
- Desbordamiento de búfer en el driver uvcvideo del kernel.
- Denegación de servicio en postfix causado por un manejo erróneo de los descriptores de archivo en algunas llamadas a sistema.
- Múltiples problemas de seguridad en xgl heredados de Xorg.
- Denegación de servicio y potencial ejecución remota de código debido a un fallo en el motor WebKit al cargar CSS.
- Actualización de seguridad de libopensc2.
- Salto de restricciones local a través de pam_mount.
- Desbordamiento de búfer en la librería bluez-libs que podría ser aprovechada para ejecutar código arbitrario por medio de dispositivos bluetooth maliciosos.

Las distintas actualizaciones para los paquetes se pueden descargar a través de las herramientas automáticas YoU (Yast Online Update), o desde el FTP de SuSE Linux: **ftp://ftp.suse.com/**

MÁS INFORMACIÓN:

- **[security-announce] SUSE Security Summary Report: SUSE-SR:2008:018**
  http://lists.opensuse.org/opensuse-security-announce/2008-09/msg00004.html

- **[security-announce] SUSE Security Summary Report: SUSE-SR:2008:019**
  http://lists.opensuse.org/opensuse-security-announce/2008-09/msg00005.html

VULNERABILIDADES EN SYMANTEC VERITAS NETBACKUP 5.X Y 6.X

Symantec Veritas Backup es un popular y completo sistema de almacenado y restauración de copias de seguridad en red.

Se han encontrado dos vulnerabilidades en Symantec Veritas NetBackup Server y Enterprise Server 5.x y 6.x que podrían ser explotadas por un atacante remoto autenticado, pero sin privilegios, para revelar información sensible, corromper cierta información del sistema o ejecutar código arbitrario.

La primera vulnerabilidad está causada por un fallo en la interfaz gráfica de administración jnbSA (Java Administration GUI) que podría ser explotado por un atacante remoto autenticado en la GUI, pero sin privilegios, para escalar privilegios y ejecutar comandos arbitarios.

La vulnerabilidad está confirmada para las versiones 5.0, 5.1, 6.0, 6.5 y 6.5.1 de Symantec Veritas NetBackup Server y Enterprise Server.

La segunda vulnerabilidad está causada por un error de validación de entrada en un control ActiveX incluido en el componente scheduler de Symantec Veritas NetBackup Server y Enterprise Server para Windows. El fallo podría dar lugar a un desbordamiento de búfer y a la utilización de métodos inseguros, y podría ser aprovechado para causar una denegación de servicio o ejecutar código arbitrario por medio de Internet Explorer.

La vulnerabilidad está confirmada para las versiones 5.1 anteriores a la 5.1 MP7, 6.0 anteriores a la 6.0 MP7, 6.5 anteriores a la 6.5.2 de Symantec Veritas NetBackup Server y Enterprise Server.

MÁS INFORMACIÓN:

- **Symantec Advisory SYM08-016: A non-privileged but authorized user could potentially leverage the NetBackup Java console to execute code with elevated privileges on the server.**
  http://seer.entsupport.symantec.com/docs/308583.htm

- **Symantec Security Advisory SYM08-007: Multiple Vulnerabilities in Scheduler component for NetBackup Server/Enterprise Server on all supported Windows Platforms.**
  http://seer.entsupport.symantec.com/docs/308669.htm

CENTRO DE CONSULTA E INVESTIGACION SOBRE SEGURIDAD DE LA INFORMACION CCISI

EMAIL:
ccisi@pcm.gob.pe

TELEFONO
2744356 – 106