

BOLETÍN DE VULNERABILIDADES
ÁUDEA, SEGURIDAD DE LA INFORMACIÓN
15 DE JULIO DE 2010

[HTTP://WWW.AUDEA.COM](http://www.audea.com)
audea@audea.com

Índice

1. Resumen de Vulnerabilidades	3
2. Boletín Detallado Vulnerabilidades	4

1. Resumen Boletín de Vulnerabilidades

- **Sistemas Operativos - MS10-042 - Crítico - 7/13/2010 - Una vulnerabilidad en el Centro de ayuda y soporte técnico podría permitir la ejecución remota de código (2229593)**
- **Sistemas Operativos - MS10-043 - Crítico - 7/13/2010 - Una vulnerabilidad en el controlador de pantalla canónico podría permitir la ejecución remota de código (2032276)**
- **Aplicaciones Usuario - MS10-044 - Crítico - 7/13/2010 - Vulnerabilidades en los controles ActiveX de Microsoft Office Access podrían permitir la ejecución remota de código (982335)**
- **Aplicaciones Usuario - MS10-045 - Importante - 7/13/2010 - Una vulnerabilidad en Microsoft Office Outlook podría permitir la ejecución remota de código (978212)**
- **Aplicaciones Usuario - 4755851 /Sun Microsystems - 7/6/2010 - Problema en el firmware de los productos Sun Fire 3800/4800/4810/6800, V1280 y Netra 1280**
- **Bases de Datos - Oracle Critical Advisory July 2010 - 7/13/2010 - Oracle Critical Patch Update Advisory**
- **Sistemas Operativos - VMSA-2010-0011 - 7/13/2010 - VMware Studio 2.1 addresses security vulnerabilities in virtual appliances created with Studio 2.0.**
- **Sistemas Operativos - SUN MICROSYSTEMS - 7/6/2010 - Una serie de servidores Sun Fire podría tener problemas en la memoria caché**
- **Sistemas Operativos - 4808603 /SUN MICROSYSTEMS - 7/6/2010 - Las CPUs a 900 Mhz de algunos equipos Sun Fire podrían sufrir bloqueos o tener un funcionamiento anómalo**
- **Sistemas Operativos - RHSA-2010:0504-01 - 7/1/2010 - Actualización del kernel de Red Hat**
- **Sistemas Operativos - RHSA-2010:0518-01 - 7/8/2010 - Actualización de seguridad en scsi-target-utils**
- **Sistemas Operativos - RHSA-2010:0519-01 - 7/8/2010 - Actualizaciones de seguridad en libtiff**
- **Sistemas Operativos - RHSA-2010:0521-01 - 7/8/2010 - Actualizaciones de seguridad en el módulo gfs-kmod**
- **Aplicaciones Usuario - RHSA-2010:0528-01 - 7/13/2010 - Actualizaciones de seguridad en avahi**
- **Sistemas Operativos - RHSA-2010:0533-01 - 7/14/2010 - Actualizaciones de seguridad en pcsc-lite**
- **Sistemas Operativos - RHSA-2010:0534-01 - 7/14/2010 - Actualizaciones de seguridad en la librería libpng10**
- **Aplicaciones Usuario - SUSE-SA:2010:025 - 7/1/2010 - Problemas de seguridad en Samba**
- **Sistemas Operativos - SUSE-SA:2010:027 - 7/5/2010 - Actualización del Kernel de SUSE:**

2. Boletín Detallado Vulnerabilidades

Sistemas Operativos - Una vulnerabilidad en el Centro de ayuda y soporte técnico podría permitir la ejecución remota de código (2229593)

Fecha: 7/13/2010

Descripción:

Esta actualización de seguridad resuelve una vulnerabilidad de la que se ha informado de forma pública en la característica Centro de ayuda y soporte técnico de Windows que se suministra con todas las ediciones compatibles de Windows XP y Windows Server 2003. Esta vulnerabilidad podría permitir la ejecución remota de código si un usuario consulta una página web especialmente diseñada mediante un explorador web o hace clic en un vínculo especialmente diseñado de un mensaje de correo electrónico. La vulnerabilidad no puede aprovecharse automáticamente mediante el correo electrónico. Un usuario debe hacer clic en un vínculo incluido en un mensaje de correo electrónico para que un ataque tenga éxito.

Productos Afectados:

Esta actualización de seguridad se considera crítica para todas las ediciones compatibles de Windows XP y baja para todas las ediciones compatibles de Windows Server 2003.

Notas:

La actualización de seguridad corrige la vulnerabilidad al modificar la manera en que los datos se validan al transferirse al Centro de ayuda y soporte técnico de Windows.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-042.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1885>

CVEs:

CVE-2010-1885

Sistemas Operativos - Una vulnerabilidad en el controlador de pantalla canónico podría permitir la ejecución remota de código (2032276)

Fecha: 7/13/2010

Descripción:

Esta actualización de seguridad resuelve una vulnerabilidad en el controlador de pantalla canónico (cdd.dll). Aunque es posible que la vulnerabilidad pudiera permitir la ejecución de código, es improbable que se realice una ejecución correcta del código debido al carácter aleatorio de la memoria. En la mayoría de los escenarios, es mucho más probable que un atacante que aprovechara esta vulnerabilidad podría provocar que el sistema afectado dejara de responder y se reiniciara automáticamente.

Productos Afectados:

Esta actualización de seguridad se considera crítica para las ediciones x64 de Windows 7 e importante para Windows Server 2008 R2.

Notas:

La actualización de seguridad corrige la vulnerabilidad al modificar la manera en que el controlador de pantalla canónico analiza la información copiada del modo usuario al modo kernel.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-043.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3678>

CVEs:

CVE-2009-3678

Aplicaciones Usuario - Vulnerabilidades en los controles ActiveX de Microsoft Office Access podrían permitir la ejecución remota de código (982335)

Fecha: 7/13/2010

Descripción:

Esta actualización de seguridad resuelve dos vulnerabilidades de las que se ha informado de forma privada en los controles ActiveX de Microsoft Office Access. Las vulnerabilidades podrían permitir la ejecución remota de código si un usuario abre un archivo de Office especialmente diseñado o consulta un sitio web que haya iniciado controles ActiveX de Access. Por tanto, los usuarios cuyas cuentas estén configuradas con pocos derechos de usuario en el sistema correrían un riesgo menor que aquellos que cuenten con derechos de usuario administrativos.

Productos Afectados:

Esta actualización de seguridad se considera crítica para las ediciones compatibles de Microsoft Office Access 2003 y Microsoft Office Access 2007.

Notas:

La actualización corrige las vulnerabilidades al actualizar determinados controles ActiveX de Access y al modificar el modo en que Microsoft Office e Internet Explorer obtienen acceso a la memoria al cargar los controles ActiveX de Access.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-044.mspx>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0814>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1881>

CVEs:

CVE-2010-0814, CVE-2010-1881

Aplicaciones Usuario - Una vulnerabilidad en Microsoft Office Outlook podría permitir la ejecución remota de código (978212)

Fecha: 7/13/2010

Descripción:

Esta actualización de seguridad resuelve una vulnerabilidad de la que se ha informado de forma privada. La vulnerabilidad podría permitir la ejecución remota de código si un usuario abre los datos adjuntos de un mensaje de correo electrónico especialmente diseñado mediante una versión afectada de Microsoft Office Outlook. Un intruso que aprovechara esta vulnerabilidad podría conseguir el mismo nivel de derechos de usuario que el usuario local. Por tanto, los usuarios cuyas cuentas estén configuradas con pocos derechos de usuario en el sistema correrían un riesgo menor que aquellos que cuenten con derechos de usuario administrativos.

Productos Afectados:

Esta actualización de seguridad se considera importante para todas las ediciones compatibles de Microsoft Outlook 2002, Microsoft Office Outlook 2003 y Microsoft Office Outlook 2007.

Notas:

La actualización corrige la vulnerabilidad al modificar la manera en que Microsoft Office Outlook comprueba los datos adjuntos de un mensaje de correo electrónico especialmente diseñado.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-045.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0266>

CVEs:

CVE-2010-0266

Aplicaciones Usuario - Problema en el firmware de los productos Sun Fire 3800/4800/4810/6800, V1280 y Netra 1280

Fecha: 7/6/2010

Descripción:

El parche 112233-08 del kernel Solaris 9 o superior no se instala en los equipos Sun Fire 3800/4800/4810/6800, Sun Fire V1280 y Netra 1280 con determinado firmware.

Productos Afectados:

Sun Fire 3800 Server

Sun Fire 4800 Server

Sun Fire 4810 Server

Sun Fire 6800 Server

Sun Fire V1280 Server

Netra 1280 Server

Notas:

Para solucionar el problema se realizarán las actualizaciones de firmware pertinentes, acorde a lo indicado en el siguiente enlace:

<http://sunsolve.sun.com/search/document.do?assetkey=1-77-1000589.1-1>

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-77-1000589.1-1>

CVEs:

Bases de Datos - Oracle Critical Patch Update Advisory

Fecha: 7/13/2010

Descripción:

Esta actualización soluciona 59 nuevos fallos de seguridad en los productos afectados, incluidos más abajo.

Productos Afectados:

- Oracle Database 11g Release 2, version 11.2.0.1
- Oracle Database 11g Release 1, version 11.1.0.7
- Oracle Database 10g Release 2, versions 10.2.0.3, 10.2.0.4
- Oracle Database 10g, version 10.1.0.5
- Oracle Database 9i Release 2, versions 9.2.0.8, 9.2.0.8DV
- Oracle TimesTen In-Memory Database, versions 7.0.6.0, 11.2.1.4.1
- Oracle Secure Backup version 10.3.0.1
- Oracle Application Server, 10gR2, version 10.1.2.3.0
- Oracle Identity Management 10g, version 10.1.4.0.1
- Oracle WebLogic Server 11gR1 releases (10.3.1, 10.3.2 and 10.3.3)
- Oracle WebLogic Server 10gR3 release (10.3.0)
- Oracle WebLogic Server 10.0 through MP2
- Oracle WebLogic Server 9.0, 9.1, 9.2 through MP3
- Oracle WebLogic Server 8.1 through SP6
- Oracle WebLogic Server 7.0 through SP7
- Oracle JRockit R28.0.0 and earlier (JDK/JRE 5 and 6)
- Oracle JRockit R27.6.6 and earlier (JDK/JRE 1.4.2, 5 and 6)
- Oracle Business Process Management, versions 5.7.3, 6.0.5, 10.3.1, 10.3.2
- Oracle Enterprise Manager Grid Control 10g Release 5, version 10.2.0.5
- Oracle Enterprise Manager Grid Control 10g Release 1, version 10.1.0.6
- Oracle E-Business Suite Release 12, versions 12.0.4, 12.0.5, 12.0.6, 12.1.1 and 12.1.2
- Oracle E-Business Suite Release 11i, versions 11.5.10, 11.5.10.2
- Oracle Transportation Manager, Versions: 5.5.05.07, 5.5.06.00, 6.0.03
- PeopleSoft Enterprise Campus Solutions, version 9.0
- PeopleSoft Enterprise CRM, versions 9.0 and 9.1
- PeopleSoft Enterprise FSCM, versions 8.9, 9.0 and 9.1
- PeopleSoft Enterprise HCM, versions 8.9, 9.0 and 9.1
- PeopleSoft Enterprise PeopleTools, versions 8.49 and 8.50
- Oracle Sun Product Suite

Notas:

Referencias en la web:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2010.html>

CVEs:

CVE-2010-0911 CVE-2010-0903 CVE-2010-0902 CVE-2010-0892 CVE-2010-0900 CVE-2010-0901 CVE-2010-0873 CVE-2010-0910 CVE-2010-0898 CVE-2010-0907 CVE-2010-0899 CVE-2010-0906 CVE-2010-0904 CVE-2010-0849 CVE-2009-3555 CVE-2010-2375 CVE-2010-2370 CVE-2010-0835 CVE-2010-0081 CVE-2010-2381 CVE-2010-2373 CVE-2010-0908 CVE-2010-0915 CVE-2010-0912 CVE-2010-0905 CVE-2010-0913 CVE-2010-0909 CVE-2010-0836 CVE-2010-2372 CVE-2010-2371 CVE-2010-2401 CVE-2010-2402 CVE-2010-2380 CVE-2010-2398 CVE-2010-2379 CVE-2010-2377 CVE-2010-2378 CVE-2010-2403 CVE-2010-0083 CVE-2008-4247 CVE-2010-0916 CVE-2010-2385 CVE-2010-2392 CVE-2010-0914 CVE-2010-2386 CVE-2010-2394 CVE-2010-2399 CVE-2010-2400 CVE-2009-3763 CVE-2009-3764 CVE-2009-3762 CVE-2010-2393 CVE-2009-0217 CVE-2010-2376 CVE-2010-2382 CVE-2010-2383 CVE-2010-2384 CVE-2010-2374 CVE-2010-2397

Sistemas Operativos - VMware Studio 2.1 addresses security vulnerabilities in virtual appliances created with Studio 2.0.

Fecha: 7/13/2010

Descripción:

Una vulnerabilidad en el Virtual Appliance Management Infrastructure (VAMI) permite la ejecución remota de comandos en Studio 2.0 o en appliances virtuales creados con Studio 2.0. Para explotar la vulnerabilidad se requiere autenticación.

Productos Afectados:

VMware Studio 2.0

Note: virtual appliances created with VMware Studio 2.0 may be affected

Notas:

Referencias en la web:

<http://www.vmware.com/security/advisories/>

CVEs:

CVE-2010-2427 CVE-2010-2667

Sistemas Operativos - Una serie de servidores Sun Fire podría tener problemas en la memoria caché

Fecha: 7/6/2010

Descripción:

Algunos servidores Sun Fire que se vendieron con un tipo de SRAM particular podría tener un problema en los componentes dando lugar a una interrupción del sistema junto con errores incorregibles en la SRAM L2.

Productos Afectados:

Sun Fire 12K Server

Sun Fire 3800 Server

Sun Fire 4800 Server

Sun Fire 4810 Server

Sun Fire 6800 Server

Sun Fire 15K Server

Sun Fire V1280 Server

Netra 1280 Server

Notas:

Solución:

Hablar con el representante de Sun correspondiente para determinar si el sistema está afectado por el problema, y realizar un reemplazo del hardware afectado.

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-77-1000386.1-1>

CVEs:

Sistemas Operativos - Las CPUs a 900 Mhz de algunos equipos Sun Fire podrían sufrir bloqueos o tener un funcionamiento anómalo

Fecha: 7/6/2010

Descripción:

Sun ha identificado el problema. Se trata de un parámetro incorrecto en los equipos Sun Fire 2800/4800/6800, Sun Fire 12K/15K, y Sun Fire V1280. Este error podría causar que se produzcan errores en la L2 SRAM, lo que podría dar lugar a bloqueos y a "domain panics".

Productos Afectados:

Sun Fire 12K Server
Sun Fire 3800 Server
Sun Fire 4800 Server
Sun Fire 4810 Server
Sun Fire 6800 Server
Sun Fire 15K Server
Sun Fire V1280 Server
Netra 1280 Server

Notas:

Solución:

Instalar el siguiente parche /Firmware

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-77-1000922.1-1>

CVEs:

Sistemas Operativos - Actualización del kernel de Red Hat

Fecha: 7/1/2010

Descripción:

Se han publicad nuevos paquetes de Red Hat enterprise Linux 5.0 que solucionan varios problemas de seguridad.

Productos Afectados:

Red Hat Enterprise Linux (v. 5 server) - i386, ia64, noarch, ppc, s390x, x86_64

Red Hat Enterprise Linux Desktop (v. 5 client) - i386, noarch, x86_64

Notas:

Se puede encontrar más información sobre las correcciones realizadas sobre estos paquetes en:

<http://kbase.redhat.com/faq/docs/DOC-11259>

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0504.html>

CVEs:

CVE-2010-0291, CVE-2010-0622, CVE-2010-1087, CVE-2010-1088, CVE-2010-1173, CVE-2010-1187, CVE-2010-1436 CVE-2010-1437, CVE-2010-1641

Sistemas Operativos - Actualización de seguridad en scsi-target-utils

Fecha: 7/8/2010

Descripción:

Se ha publicado un paquete actualizado de scsi-target-utils que soluciona varios problemas de seguridad. Se encuentra disponible para Red Hat Linux 5.

Productos Afectados:

RHEL Cluster-Storage (v. 5 server) - i386, ia64, ppc, x86_64

Notas:

Se puede encontrar más información sobre el paquete de actualización en:

Referencias en la web:

<http://kbase.redhat.com/faq/docs/DOC-11259>

CVEs:

CVE-2010-2221

Sistemas Operativos - Actualizaciones de seguridad en libtiff

Fecha: 7/8/2010

Descripción:

Se ha publicado un paquete de actualización de la librería libtiff. Este paquete soluciona muchas vulnerabilidades, que provocaban buffer overflows de cálculo a través de la apertura de un fichero TIFF especialmente diseñado. Posteriormente, el atacante podría ejecutar código o bloquear el equipo.

Productos Afectados:

RHEL Desktop Workstation (v. 5 client) - i386, x86_64

Red Hat Enterprise Linux (v. 5 server) - i386, ia64, ppc, s390x, x86_64

Red Hat Enterprise Linux AS version 4 - i386, ia64, ppc, s390, s390x, x86_64

Red Hat Enterprise Linux Desktop (v. 5 client) - i386, x86_64

Red Hat Enterprise Linux Desktop version 4 - i386, x86_64

Red Hat Enterprise Linux ES version 4 - i386, ia64, x86_64

Red Hat Enterprise Linux WS version 4 - i386, ia64, x86_64

Notas:

Se puede encontrar más información sobre el paquete de actualización en:

<http://kbase.redhat.com/faq/docs/DOC-11259>

Referencias en la web:

<http://kbase.redhat.com/faq/docs/DOC-11259>

<https://rhn.redhat.com/errata/RHSA-2010-0519.html>

CVEs:

CVE-2010-1411, CVE-2010-2481, CVE-2010-2483, CVE-2010-2595 CVE-2010-2597

Sistemas Operativos - Actualizaciones de seguridad en el módulo gfs-kmod

Fecha: 7/8/2010

Descripción:

Se ha encontrado un error en la implementación de la función `gfs_lock()`. El código de "GFS Locking" podría saltarse la operación de bloqueo en los ficheros que tengan establecido el bit `S_ISGID`. Un usuario local sin privilegios que tenga un sistema de ficheros GFS montado podría utilizar este error para causar una situación de "kernel panic".

Productos Afectados:

Red Hat Enterprise Linux

Notas:

Se puede encontrar información detallada sobre la actualización descrita en:

<http://kbase.redhat.com/faq/docs/DOC-11259>

Referencias en la web:

<http://kbase.redhat.com/faq/docs/DOC-11259>

<https://rhn.redhat.com/errata/RHSA-2010-0521.html>

CVEs:

CVE-2010-0727

Aplicaciones Usuario - Actualizaciones de seguridad en avahi

Fecha: 7/13/2010

Descripción:

Se han publicado varios paquetes actualizados de avahi que solucionan dos vulnerabilidades de seguridad. Estos paquetes se encuentran disponibles para Red Hat Enterprise Linux 5. Las vulnerabilidades resueltas son las siguientes:

- Se ha encontrado un error en la forma en la que el demonio Avahi procesa los paquetes DNS Multicast.
- Se ha encontrado un error en la forma en la que se reciben paquetes unicast mDNS.

Ambos errores podrían generar un gran tráfico de red que consumiría mucha CPU y ancho de banda de la red.

Productos Afectados:

RHEL Desktop Workstation (v. 5 client) - i386, x86_64

Red Hat Enterprise Linux (v. 5 server) - i386, ia64, ppc, s390x, x86_64

Red Hat Enterprise Linux Desktop (v. 5 client) - i386, x86_64

Notas:

Se puede encontrar más información sobre las actualizaciones en:

<http://kbase.redhat.com/faq/docs/DOC-11259>

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0528.html>

<http://kbase.redhat.com/faq/docs/DOC-11259>

CVEs:

CVE-2009-0758 CVE-2010-2244

Sistemas Operativos - Actualizaciones de seguridad en pcsc-lite

Fecha: 7/14/2010

Descripción:

Se han encontrado varias vulnerabilidades de buffer overflow en el demonio pcscd. Un usuario local podría crear una petición especialmente diseñada que podría causar que el demonio de pcscd se bloquee, o incluso se podría permitir la ejecución remota de código.

Productos Afectados:

RHEL Desktop Workstation (v. 5 client) - i386, x86_64

Red Hat Enterprise Linux (v. 5 server) - i386, ia64, ppc, x86_64

Red Hat Enterprise Linux Desktop (v. 5 client) - i386, x86_64

Notas:

Se puede encontrar más información sobre la actualización en:

<http://kbase.redhat.com/faq/docs/DOC-11259>

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0533.html>

<http://kbase.redhat.com/faq/docs/DOC-11259>

CVEs:

CVE-2009-4901, CVE-2010-0407

Sistemas Operativos - Actualizaciones de seguridad en la librería libpng10

Fecha: 7/14/2010

Descripción:

Se han publicado paquetes actualizados de las librerías libpng10 para Red Hat Enterprise Linux 3, 4 y 5.

Estos paquetes solucionan las siguientes vulnerabilidades:

-Corrupción de memoria al utilizar la librería libpng con su método de lectura progresiva decodificando determinadas imágenes PNG.

-Denegación de Servicio al utilizar libpng para archivos con una alta compresión

Productos Afectados:

RHEL Desktop Workstation (v. 5 client) - i386, x86_64

Red Hat Desktop version 3 - i386, x86_64

Red Hat Enterprise Linux (v. 5 server) - i386, ia64, ppc, s390x, x86_64

Red Hat Enterprise Linux AS version 3 - i386, ia64, ppc, s390, s390x, x86_64

Red Hat Enterprise Linux AS version 4 - i386, ia64, ppc, s390, s390x, x86_64

Red Hat Enterprise Linux Desktop (v. 5 client) - i386, x86_64

Red Hat Enterprise Linux Desktop version 4 - i386, x86_64

Red Hat Enterprise Linux ES version 3 - i386, ia64, x86_64

Red Hat Enterprise Linux ES version 4 - i386, ia64, x86_64

Red Hat Enterprise Linux WS version 3 - i386, ia64, x86_64

Red Hat Enterprise Linux WS version 4 - i386, ia64, x86_64

Notas:

Se puede encontrar más información sobre los paquetes de actualización en:

<http://kbase.redhat.com/faq/docs/DOC-11259>

Referencias en la web:

<http://kbase.redhat.com/faq/docs/DOC-11259>

<https://rhn.redhat.com/errata/RHSA-2010-0534.html>

CVEs:

CVE-2009-2042, CVE-2010-0205, CVE-2010-1205, CVE-2010-2249

Aplicaciones Usuario - Problemas de seguridad en Samba

Fecha: 7/1/2010

Descripción:

Se han publicado actualizaciones de seguridad que solventan las siguientes vulnerabilidades:

-Vulnerabilidad de buffer overrun en el código chain_repalý de las versiones 3.3.x y anteriores, el cual podría utilizarse para bloquear el servidor samba o ejecutar código potencialmente peligroso.

-Cuando se establece un punto de montaje, el mount.cifs no cambia durante el montaje.

Productos Afectados:

openSUSE 11.0

openSUSE 11.1

SUSE SLES 9

Open Enterprise Server

Novell Linux POS 9

SLE SDK 10 SP3

SUSE Linux Enterprise Desktop 10 SP3

SUSE Linux Enterprise Server 10 SP3

SUSE Linux Enterprise Software Development Kit 11

SUSE Linux Enterprise Desktop 11

SUSE Linux Enterprise Server 11

Notas:

Se puede encontrar más información sobre la actualización en:

http://www.novell.com/linux/security/advisories/2010_25_samba.html

Referencias en la web:

http://www.novell.com/linux/security/advisories/2010_25_samba.html

CVEs:

CVE-2010-0787, CVE-2010-2063

Sistemas Operativos - Actualización del Kernel de SUSE:

Fecha: 7/5/2010

Descripción:

Se han publicado la actualización de kernel SUSE Linux Enterprise 11 Service Pack 1 (versión 2.6.32.13), que contiene múltiples parches y actualizaciones de seguridad.

CVE-2010-1173: 2010-1173: La función `sctp_process_unk_param` en `net/sctp/sm_make_chunk.c` cuando SCTP está habilitado, permite a los atacantes remotos provocar Denegaciones de Servicio mediante un paquete SCTPChunkunit, que contiene varios parámetros inválidos que requieren una gran cantidad de datos de error.

Productos Afectados:

SUSE Linux Enterprise Desktop 11 SP1

SUSE Linux Enterprise Server 11 SP1

SUSE Linux Enterprise High Availability Extension 11 SP1

Notas:

Se puede obtener más información sobre la actualización en:

http://www.novell.com/linux/security/advisories/2010_27_kernel.html

Referencias en la web:

http://www.novell.com/linux/security/advisories/2010_27_kernel.html

CVEs:

CVE-2010-1173

