

**BOLETÍN DE VULNERABILIDADES**  
**ÁUDEA, SEGURIDAD DE LA INFORMACIÓN**  
**15 DE MAYO DE 2010**

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

## Índice

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

## 1. Resumen Boletín de Vulnerabilidades

- **Sistemas Operativos - RHSA-2010:0386-01 - 5/3/2010 - Sexto mes en el que se notifica el fin de vida del producto Red Hat Enterprise Linux 3.**
- **Sistemas Operativos - RHSA-2010:0394-01 - 5/5/2010 - Actualización del Kernel de Red Hat Enterprise Linux**
- **Sistemas Operativos - RHSA-2010:0398-01 - 5/6/2010 - Publicación de paquetes del Kernel Actualizados**
- **Sistemas Operativos - SUSE-SA:2010:023 - 5/6/2010 - Actualizaciones de seguridad en el kernel de SUSE**
- **Aplicaciones Usuario - SUSE-SR:2010:011 - 5/10/2010 - Actualizaciones de seguridad en varios programas de SUSE**
- **Sistemas Operativos - Sun Microsystems weekly summary report - 5/8/2010 - Resumen semanal de Vulnerabilidades en los productos de Sun Microsystems**
- **Sistemas Operativos - MS10-030 – Crítico - 5/11/2010 - Una vulnerabilidad en Outlook Express y Windows Mail podría permitir la ejecución remota de código (978542)**
- **Aplicaciones Usuario - MS10-031 - Crítico - 5/11/2010 - Una vulnerabilidad en Microsoft Visual Basic para Aplicaciones podría permitir la ejecución remota de código (978213)**
- **Aplicaciones Usuario - APSB10-11 Importante - 5/11/2010 - Actualización de seguridad disponible para ColdFusion**
- **Aplicaciones Usuario - APSB10-12 Crítico - 5/11/2010 - Actualización de seguridad disponible para Shockwave Player**
- **Aplicaciones Usuario - 6239342, 6240424, 6240422 /Sun Microsystems - 5/13/2010 - Vulnerabilidad de Cross Site Scripting en las aplicaciones Sun ONE y Sun Java System**
- **Sistemas Operativos - Novell Updates - 5/14/2010 - Publicadas actualizaciones de varios módulos de SUSE Linux**
- **Aplicaciones Usuario - DSA-2040-1 /Debian - 5/2/2010 - Vulnerabilidad en squidguard**
- **Sistemas Operativos - DSA-2042-1 /Debian - 5/5/2010 - Vulnerabilidad en iscitarget**
- **Aplicaciones Usuario - DSA-2043-1-DSA-2044-1 /Debian - 5/11/2010 - Desbordamiento de enteros en vlc**
- **Aplicaciones Usuario - DSA-2045-1 - 5/11/2010 - Desbordamiento de enteros en libtheora**
- **Servicios (ftp, www, dns, etc.) - DSA-2046-1 /Debian - 5/13/2010 - Vulnerabilidad en phpgroupware**

## 2. Boletín Detallado Vulnerabilidades

**Sistemas Operativos - Sexto mes en el que se notifica el fin de vida del producto Red Hat Enterprise Linux 3.**

**Fecha:** 5/3/2010

**Descripción:**

Este es el sexto mes que se notifica el fin de vida de los productos Red Hat Enterprise Linux 3.

La fecha oficial en la que se dejará de dar soporte a la gama de productos Red Hat Linux Enterprise 3 es el 31 de Octubre de 2010.

Concretamente, los productos a los que se dejará de dar soporte son:

- Red Hat Enterprise Linux AS 3
- Red Hat Enterprise Linux ES 3
- Red Hat Enterprise Linux WS 3
- Red Hat Enterprise Linux Extras 3
- Red Hat Desktop 3
- Red Hat Global File System 3
- Red Hat Cluster Suite 3

**Productos Afectados:**

Red Hat Desktop version 3 - i386, x86\_64

Red Hat Enterprise Linux AS version 3 - i386, ia64, ppc, s390, s390x, x86\_64

Red Hat Enterprise Linux ES version 3 - i386, ia64, x86\_64

Red Hat Enterprise Linux WS version 3 - i386, ia64, x86\_64

**Notas:**

Se recomienda planificar una migración a la versión 5 de los productos Red Hat.

**Referencias en la web:**

<https://rhn.redhat.com/errata/RHSA-2010-0386.html>

**CVEs:**

## Sistemas Operativos - Actualización del Kernel de Red Hat Enterprise Linux

Fecha: 5/5/2010

### Descripción:

Se ha publicado una actualización del Kernel de Red Hat Linux, en el que se han solucionado las siguientes vulnerabilidades:

-RHSA-2009:1024: Error en la implementación de "ptrace" de los sistemas Itanium. La función `ptrace_check_attach()` no se invoca durante determinadas peticiones `ptrace`. En determinadas circunstancias, un usuario local sin privilegios podría utilizar este problema para invocar a `ptrace()` en un proceso que no le pertenece, obteniendo control sobre el mismo.

-Error en el "kernel's Unidirectional Lightweight Encapsulation". Un atacante remoto podría enviar un frame ISO MPEG-2 Transport Stream al sistema objetivo, provocando una Denegación de Servicio.

-Error de tipo "use after free" en el proceso `rcv_state_process()` de la implementación del protocolo TCP/IP. Si un sistema que utiliza IPV6 tiene la opción `IPV6_RECVPKTINFO` establecida en un socket que escucha, un atacante remoto podría enviar un paquete IPV6 al sistema, causando una situación de "kernel panic".

-Se ha encontrado un error en la función `azx_position_ok()` el driver "Intel High Definition Audio", que podría permitir realizar una división entre 0. Un usuario no privilegiado podría aprovechar esta vulnerabilidad para causar una situación de Denegación de Servicio.

-Se ha encontrado un problema de fuga de información en la implementación USB del kernel. Determinados errores USB podrían resultar en un buffer sin inicializar del kernel que se envía al "user-space". Un atacante con acceso físico al sistema objetivo podría utilizar esta vulnerabilidad para provocar una fuga de información.

### Productos Afectados:

Red Hat Enterprise Linux AS version 4 - i386, ia64, noarch, ppc, s390, s390x, x86\_64

Red Hat Enterprise Linux Desktop version 4 - i386, noarch, x86\_64

Red Hat Enterprise Linux ES version 4 - i386, ia64, noarch, x86\_64

Red Hat Enterprise Linux WS version 4 - i386, ia64, noarch, x86\_64

### Notas:

Más información sobre las vulnerabilidades solventadas con la nueva actualización en:

<https://rhn.redhat.com/errata/RHSA-2010-0394.html>

**Referencias en la web:**

<https://rhn.redhat.com/errata/RHSA-2010-0394.html>

**CVEs:**

CVE-2010-0729 CVE-2010-1083 CVE-2010-1085 CVE-2010-1086 CVE-2010-1188

## Sistemas Operativos - Publicación de paquetes del Kernel Actualizados

Fecha: 5/6/2010

### Descripción:

Los nuevos paquetes solucionan varias vulnerabilidades. A continuación se nombren algunas de las más importantes:

-Problema en el la implementación de "Unidirectional Lightweight Encapsulation". Un atacante remoto podría enviar un frame ISO MPEG-2 Transport Stream especialmente diseñado, causando una Denegación de Servicio (bucle infinito).

-Se ha descubierto un problema en los sistemas AMD 64 en el que el kernel no asegura que el intérprete ELF esté disponible tras realizar una llamada a la macro SET\_PERSONALITY. Un atacante local podría utilizar este problema para causar una Denegación de Servicio al ejecutar una aplicación de 32 bits que permite la ejecución de una aplicación de 64 bits.

-Se ha encontrado un problema en el decodificador de instrucciones Memory Mapped I/O (MMIO) de la implementación Xen hypervisor. Un usuario invitado sin privilegios podría utilizar este problema para hacer que el hypervisor pueda provocar un bloqueo en el equipo al emularse una determinada instrucción.

-Se ha encontrado un error en la función azx\_position\_ok() el driver "Intel High Definition Audio", que podría permitir realizar una división entre 0. Un usuario no privilegiado podría aprovechar esta vulnerabilidad para causar una situación de Denegación de Servicio.

-En algunos casos, al arrancar un sistema con el parámetro "iommu=on", se produce una situación de hypervisor panic.

### 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:

Más información en:

<https://rhn.redhat.com/errata/RHSA-2010-0398.html>

### Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0398.html>

### CVEs:

CVE-2010-0307 CVE-2010-0410 CVE-2010-0730 CVE-2010-1085 CVE-2010-1086

## Sistemas Operativos - Actualizaciones de seguridad en el kernel de SUSE

Fecha: 5/6/2010

### Descripción:

A continuación se describen algunos problemas solventados con las actualizaciones del kernel:

CVE-2009-4537: drivers/net/r8169.c in the r8169 driver in the Linux kernel does not properly check the size of an Ethernet frame that exceeds the MTU, which allows remote attackers to (1) cause a denial of service (temporary network outage) via a packet with a crafted size, in conjunction with certain packets containing A characters and certain packets containing E characters; or (2) cause a denial of service (system crash) via a packet with a crafted size, in conjunction with certain packets containing 'O' characters, related to the value of the status register and erroneous behavior associated with the RxMaxSize register.

CVE-2010-1086: The ULE decapsulation functionality in drivers/media/dvb/dvb-core/dvb\_net.c in dvb-core in the Linux kernel earlier allows attackers to cause a denial of service (infinite loop) via a crafted MPG2-TS frame, related to an invalid Payload Pointer ULE.

CVE-2010-1088: fs/namei.c in Linux kernel does not always follow NFS automount "symlinks," which allows attackers to have an unknown impact, related to LOOKUP\_FOLLOW.

CVE-2009-4020: Stack-based buffer overflow in the hfs subsystem in the Linux kernel allows remote attackers to have an unspecified impact via a crafted Hierarchical File System (HFS) filesystem, related to the hfs\_readdir function in fs/hfs/dir.c.

CVE-2010-1083: The processcompl\_compat function in drivers/usb/core/devio.c in the Linux kernel does not clear the transfer buffer before returning to user space when a USB command fails, which might make it easier for physically proximate attackers to obtain sensitive information (kernel memory).

CVE-2010-0410: drivers/connector/connector.c in the Linux kernel allows local users to cause a denial of service (memory consumption and system crash) by sending the kernel many NETLINK\_CONNECTOR messages.

### Productos Afectados:

SLE SDK 10 SP2

SUSE Linux Enterprise Desktop 10 SP2

SUSE Linux Enterprise Server 10 SP2

### Notas:

Se puede encontrar más información y descargas de paquetes actualizados en la URL:

[http://www.novell.com/linux/security/advisories/2010\\_23\\_kernel.html](http://www.novell.com/linux/security/advisories/2010_23_kernel.html)

**Referencias en la web:**

[http://www.novell.com/linux/security/advisories/2010\\_23\\_kernel.html](http://www.novell.com/linux/security/advisories/2010_23_kernel.html)

**CVEs:**

CVE-2009-4020, CVE-2009-4537, CVE-2010-0410, CVE-2010-1083, CVE-2010-1086, CVE-2010-1088

## **Aplicaciones Usuario - Actualizaciones de seguridad en varios programas de SUSE**

**Fecha:** 5/10/2010

### **Descripción:**

Se han solventado diversos problemas de seguridad encontrados en los siguientes programas:

#### **Solved Security Vulnerabilities:**

- dovecot12
- cacti
- java-1\_6\_0-openjdk
- irssi
- tar
- fuse
- apache2
- libmysqlclient-devel
- cpio
- moodle
- libmikmod
- libicecore
- evolution-data-server
- libpng/libpng-devel
- libesmtp

#### **Productos Afectados:**

##### **Aplicaciones de SUSE:**

- dovecot12
  - cacti
  - java-1\_6\_0-openjdk
  - irssi
  - tar
  - fuse
  - apache2
  - libmysqlclient-devel
  - cpio
  - moodle
  - libmikmod
  - libicecore
  - evolution-data-server
  - libpng/libpng-devel

- libesntp

**Notas:**

Se puede encontrar más información en la URL:

[http://www.novell.com/linux/security/advisories/2010\\_11\\_sr.html](http://www.novell.com/linux/security/advisories/2010_11_sr.html)

**Referencias en la web:**

[http://www.novell.com/linux/security/advisories/2010\\_11\\_sr.html](http://www.novell.com/linux/security/advisories/2010_11_sr.html)

**CVEs:**

CVE-2008-7247, CVE-2009-0547, CVE-2009-1955,  
CVE-2009-2412, CVE-2009-2625, CVE-2009-3297,  
CVE-2009-3555, CVE-2009-3560, CVE-2009-3720,  
CVE-2009-3995, CVE-2009-3996, CVE-2009-4019,  
CVE-2009-4028, CVE-2009-4030, CVE-2010-0082,  
CVE-2010-0084, CVE-2010-0085, CVE-2010-0088,  
CVE-2010-0091, CVE-2010-0092, CVE-2010-0093,  
CVE-2010-0094, CVE-2010-0095, CVE-2010-0205,  
CVE-2010-0624, CVE-2010-0745, CVE-2010-0789,  
CVE-2010-0837, CVE-2010-0838, CVE-2010-0840,  
CVE-2010-0845, CVE-2010-0847, CVE-2010-0848,  
CVE-2010-1155, CVE-2010-1156, CVE-2010-1192,  
CVE-2010-1194, CVE-2010-1431, CVE-2010-1613,  
CVE-2010-1614, CVE-2010-1615, CVE-2010-1616,  
CVE-2010-1617, CVE-2010-1618, CVE-2010-1619

## **Sistemas Operativos - Resumen semanal de Vulnerabilidades en los productos de Sun Microsystems**

**Fecha:** 5/8/2010

### **Descripción:**

2 de Mayo: Vulnerabilidad en HIPER-Oracle StorageTek HSC: El servicio termina de forma inesperada mostrano el error: ABEND U1096 RC=1729070D.

8 de Mayo: Al instalar la actualización KB980232 en los sistemas windows que acceden a un sistema NAS ST5210/5220/5310/5320 puede provocar una pérdida de accesos a ficehro o de descriptores de fichero.

### **Productos Afectados:**

-HIPER- Oracle Storagetek HSC

-Equipos windows que utilicen un sistema NAS ST5210/5220/5310/5320

### **Notas:**

Se puede encontrar más información en:

<http://www.oracle.com/technology/deploy/security/alerts.htm>

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-275470-1>

### **Referencias en la web:**

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-280030-1>

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-279830-1>

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-275470-1>

### **CVEs:**

## **Sistemas Operativos - Una vulnerabilidad en Outlook Express y Windows Mail podría permitir la ejecución remota de código (978542)**

**Fecha:** 5/11/2010

### **Descripción:**

Esta actualización de seguridad crítica resuelve una vulnerabilidad de la que se ha informado de forma privada en Outlook Express, Windows Mail y Windows Live Mail. La vulnerabilidad podría permitir la ejecución remota de código si un usuario visita un servidor de correo electrónico malintencionado. 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 crítica para Microsoft Outlook Express en todas las ediciones compatibles de Microsoft Windows 2000, Windows XP y Windows Server 2003, y para Windows Mail en todas las ediciones compatibles de Windows Vista y Windows Server 2008. Esta actualización de seguridad se considera importante para Windows Live Mail en todas las ediciones compatibles de Windows XP, Windows Vista, Windows Server 2008, Windows 7 y Windows Server 2008 R2, y para Windows Mail en todas las ediciones compatibles de Windows 7 y Windows Server 2008 R2.

### **Notas:**

La actualización de seguridad corrige la vulnerabilidad al validar correctamente las respuestas del servidor de correo electrónico.

### **Referencias en la web:**

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-030.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0816>

### **CVEs:**

CVE-2010-0816

## **Aplicaciones Usuario - Una vulnerabilidad en Microsoft Visual Basic para Aplicaciones podría permitir la ejecución remota de código (978213)**

Fecha: 5/11/2010

### **Descripción:**

Esta actualización de seguridad resuelve una vulnerabilidad de la que se ha informado de forma privada en Microsoft Visual Basic para Aplicaciones. La vulnerabilidad podría permitir la ejecución remota de código si una aplicación host abre y pasa un archivo especialmente diseñado al módulo de tiempo de ejecución de Visual Basic para Aplicaciones. Si un usuario inicia sesión con derechos de usuario administrativos, un intruso que aprovechara esta vulnerabilidad podría lograr el control completo de un sistema afectado. De esta forma, un intruso podría instalar programas; ver, cambiar o eliminar datos; o crear cuentas nuevas con todos los derechos de usuario. 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 todas las versiones compatibles del SDK de Microsoft Visual Basic para Aplicaciones y las aplicaciones de terceros que usan Microsoft Visual Basic para Aplicaciones. Esta actualización de seguridad también se considera importante para todas las ediciones compatibles de Microsoft Office XP, Microsoft Office 2003 y 2007 Microsoft Office System.

### **Notas:**

La actualización corrige la vulnerabilidad al modificar la forma en que Visual Basic para Aplicaciones busca los controles ActiveX incrustados en los documentos.

### **Referencias en la web:**

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-031.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0815>

### **CVEs:**

CVE-2010-0815

## **Aplicaciones Usuario - Actualización de seguridad disponible para ColdFusion**

**Fecha:** 5/11/2010

### **Descripción:**

Se han detectado vulnerabilidades importantes en ColdFusion 8.0, 8.0.1, 9.0 y versiones anteriores para Windows, Macintosh y UNIX. Estas vulnerabilidades podrían llevar a cross site scripting y revelación de información.

### **Productos Afectados:**

ColdFusion 8.0, 8.0.1, 9.0 y versiones anteriores para Windows, Macintosh y UNIX

### **Notas:**

Adobe recomienda a los usuarios de ColdFusion afectados actualizar su instalación utilizando las instrucciones facilitadas en el siguiente enlace: [http://kb2.adobe.com/cps/841/cpsid\\_84102.html](http://kb2.adobe.com/cps/841/cpsid_84102.html)

### **Referencias en la web:**

<http://www.adobe.com/support/security/bulletins/apsb10-11.html>

<http://cve.mitre.org>

### **CVEs:**

CVE-2009-3467, CVE-2010-1293, CVE-2010-1294

## **Aplicaciones Usuario - Actualización de seguridad disponible para Shockwave Player**

**Fecha:** 5/11/2010

### **Descripción:**

Se han identificado vulnerabilidades críticas en Adobe Shockwave Player 11.5.6.606 y versiones anteriores en los sistemas operativos Windows y Macintosh.

### **Productos Afectados:**

Shockwave Player 11.5.6.606 y versiones anteriores para Windows y Macintosh.

### **Notas:**

Adobe recomienda a los usuarios de Adobe Shockwave Player 11.5.6.606 y versiones anteriores actualizar a la última versión 11.5.7.609, disponible aquí: <http://get.adobe.com/shockwave/>

### **Referencias en la web:**

<http://www.adobe.com/support/security/bulletins/apsb10-12.html>

<http://cve.mitre.org>

### **CVEs:**

CVE-2010-0127, CVE-2010-0128, CVE-2010-0129, CVE-2010-0130, CVE-2010-0986, CVE-2010-0987, CVE-2010-1280, CVE-2010-1281, CVE-2010-1282, CVE-2010-1283, CVE-2010-1284, CVE-2010-1286, CVE-2010-1287, CVE-2010-1288, CVE-2010-1289, CVE-2010-1290, CVE-2010-1291, CVE-2010-1292

## Aplicaciones Usuario - Vulnerabilidad de Cross Site Scripting en las aplicaciones Sun ONE y Sun Java System

Fecha: 5/13/2010

### Descripción:

Se ha encontrado una vulnerabilidad de Cross Site Scripting (XSS) en múltiples versiones del producto Sun Java System Web Server y Sun Java System Application Server. Esta vulnerabilidad podría permitir a un usuario local o remoto sin privilegios robar información sobre las cookies, robar sesiones, o causar pérdida de la privacidad de los datos entre el cliente y el servidor.

### Productos Afectados:

Sun Java System Application Server Standard Edition 7 2004Q2

Sun ONE Application Server 7, Standard Edition

Sun Java System Web Server 6.1 Service Pack 4

Sun ONE Web Server 6.0 Service Pack 9

Sun Java System Application Server Enterprise Edition 7 2004Q2

Sun ONE Application Server 7, Platform Edition

### Notas:

Solución: Actualizar el software a las siguientes versiones:

Sun ONE Web Server 6.0 Service Pack 10 or later at

<http://www.sun.com/download/products.xml?id=43a84f89>

Sun Java System Web Server 6.1 Service Pack 5 or later at

<http://www.sun.com/download/products.xml?id=434aec1d>

(International version at <http://www.sun.com/download/products.xml?id=43c43041>)

Sun ONE Application Server 7 Platform Edition Update 7 or later at

<http://www.sun.com/download/products.xml?id=42ae3178>

Sun ONE Application Server 7 Standard Edition Update 7 or later at

<http://www.sun.com/download/products.xml?id=42ae317c>

Sun Java System Application Server 7 2004Q2 Standard Edition Update 3 or later at

<http://www.sun.com/download/products.xml?id=427fe06d>

Sun Java System Application Server 7 2004Q2 Enterprise Edition Update 3 or later at

<http://javashoplmsun.com/ECom/docs/Welcome.jsp?StoreId=8&PartDetailId=SJAS72004Q2U3-EE-OTH-G-ES>

**Referencias en la web:**

<http://sunsolve.sun.com/search/document.do?assetkey=1-77-1000016.1-1>

**CVEs:**

## Sistemas Operativos - Publicadas actualizaciones de varios módulos de SUSE Linux

Fecha: 5/14/2010

### Descripción:

Se han publicado actualizaciones que solucionan diversos problemas presentes en los paquetes:

- hal
- util-linux
- supportutils
- YaST2
- Evolution-data-server
- yast2-gtk
- gconf2-branding-hp-cnb
- grub
- python
- TeX
- iwlagn-2-6-27-kmp-default
- memcached
- OES Linux servers

### Productos Afectados:

HAL:

- SUSE Linux Enterprise Desktop 11 for x86-64
- SUSE Linux Enterprise Desktop 11 for x86
- SUSE Linux Enterprise Server 11 for x86-64
- SUSE Linux Enterprise Server 11 for x86
- SUSE Linux Enterprise Server 11 for s390x
- SUSE Linux Enterprise Server 11 for ppc
- SUSE Linux Enterprise Server 11 for ia64
- SUSE Linux Enterprise Software Development Kit 11 for x86-64
- SUSE Linux Enterprise Software Development Kit 11 for x86
- SUSE Linux Enterprise Software Development Kit 11 for s390x
- SUSE Linux Enterprise Software Development Kit 11 for ppc
- SUSE Linux Enterprise Software Development Kit 11 for ia64

Util-linux:

- SUSE Linux Enterprise Desktop 10 SP3 for x86-64

SUSE Linux Enterprise Desktop 10 SP3 for x86  
SUSE Linux Enterprise Server 10 SP3 for x86-64  
SUSE Linux Enterprise Server 10 SP3 for x86-64  
SUSE Linux Enterprise Server 10 SP3 for x86  
SUSE Linux Enterprise Server 10 SP3 for x86  
SUSE Linux Enterprise Server 10 SP3 for s390x  
SUSE Linux Enterprise Server 10 SP3 for s390x  
SUSE Linux Enterprise Server 10 SP3 for ppc  
SUSE Linux Enterprise Server 10 SP3 for ppc  
SUSE Linux Enterprise Server 10 SP3 for ia64  
SUSE Linux Enterprise Server 10 SP3 for ia64

Supportutils:

SUSE Linux Enterprise Desktop 11 for x86-64  
SUSE Linux Enterprise Desktop 11 for x86  
SUSE Linux Enterprise Desktop 10 SP3 for x86-64  
SUSE Linux Enterprise Desktop 10 SP3 for x86  
SUSE Linux Enterprise Server 11 for x86-64  
SUSE Linux Enterprise Server 11 for x86  
SUSE Linux Enterprise Server 11 for s390x  
SUSE Linux Enterprise Server 11 for ppc  
SUSE Linux Enterprise Server 11 for ia64  
SUSE Linux Enterprise Server 10 SP3 for x86-64  
SUSE Linux Enterprise Server 10 SP3 for x86  
SUSE Linux Enterprise Server 10 SP3 for s390x  
SUSE Linux Enterprise Server 10 SP3 for ppc  
SUSE Linux Enterprise Server 10 SP3 for ia64

YaST2:

SUSE Linux Enterprise Desktop 11 for x86-64  
SUSE Linux Enterprise Desktop 11 for x86  
SUSE Linux Enterprise Server 11 for x86-64  
SUSE Linux Enterprise Server 11 for x86  
SUSE Linux Enterprise Server 11 for s390x  
SUSE Linux Enterprise Server 11 for ppc  
SUSE Linux Enterprise Server 11 for ia64

SUSE Linux Enterprise Software Development Kit 11 for x86-64  
SUSE Linux Enterprise Software Development Kit 11 for x86  
SUSE Linux Enterprise Software Development Kit 11 for s390x  
SUSE Linux Enterprise Software Development Kit 11 for ppc  
SUSE Linux Enterprise Software Development Kit 11 for ia64  
WebYaST [Appliance - Tools] for x86-64  
WebYaST [Appliance - Tools] for x86

Evolution-data-server:

SUSE Linux Enterprise Desktop 10 SP3 for x86-64  
SUSE Linux Enterprise Desktop 10 SP3 for x86  
SUSE Linux Enterprise Server 10 SP3 for x86-64  
SUSE Linux Enterprise Server 10 SP3 for x86-64  
SUSE Linux Enterprise Server 10 SP3 for x86  
SUSE Linux Enterprise Server 10 SP3 for x86  
SUSE Linux Enterprise Server 10 SP3 for s390x  
SUSE Linux Enterprise Server 10 SP3 for s390x  
SUSE Linux Enterprise Server 10 SP3 for ppc  
SUSE Linux Enterprise Server 10 SP3 for ppc  
SUSE Linux Enterprise Server 10 SP3 for ia64  
SUSE Linux Enterprise Server 10 SP3 for ia64

Yast2-gtk

SUSE Linux Enterprise Desktop 11 for x86-64  
SUSE Linux Enterprise Desktop 11 for x86  
SUSE Linux Enterprise Software Development Kit 11 for x86-64  
SUSE Linux Enterprise Software Development Kit 11 for x86  
SUSE Linux Enterprise Software Development Kit 11 for s390x  
SUSE Linux Enterprise Software Development Kit 11 for ppc  
SUSE Linux Enterprise Software Development Kit 11 for ia64

Gconf2-branding-hp-cnb:

SUSE Linux Enterprise Desktop 11 for x86-64  
SUSE Linux Enterprise Desktop 11 for x86

Grub:

SUSE Linux Enterprise Desktop 10 SP3 for x86-64  
SUSE Linux Enterprise Desktop 10 SP3 for x86  
SUSE Linux Enterprise Server 10 SP3 for x86-64  
SUSE Linux Enterprise Server 10 SP3 for x86-64  
SUSE Linux Enterprise Server 10 SP3 for x86  
SUSE Linux Enterprise Server 10 SP3 for x86

Python:

Linux Point of Service 9 for x86  
Open Enterprise Server (Linux) for x86  
SUSE Linux Enterprise Desktop 11 for x86-64  
SUSE Linux Enterprise Desktop 11 for x86  
SUSE Linux Enterprise Desktop 10 SP3 for x86-64  
SUSE Linux Enterprise Desktop 10 SP3 for x86  
SUSE Linux Enterprise Server 11 for x86-64  
SUSE Linux Enterprise Server 11 for x86  
SUSE Linux Enterprise Server 11 for s390x  
SUSE Linux Enterprise Server 11 for ppc  
SUSE Linux Enterprise Server 11 for ia64  
SUSE Linux Enterprise Server 10 SP3 for x86-64  
SUSE Linux Enterprise Server 10 SP3 for x86  
SUSE Linux Enterprise Server 10 SP3 for s390x  
SUSE Linux Enterprise Server 10 SP3 for ppc  
SUSE Linux Enterprise Server 10 SP3 for ia64  
SUSE Linux Enterprise Server 9 for x86-64  
SUSE Linux Enterprise Server 9 for x86  
SUSE Linux Enterprise Server 9 for s390x  
SUSE Linux Enterprise Server 9 for s390  
SUSE Linux Enterprise Server 9 for ppc  
SUSE Linux Enterprise Server 9 for ia64  
SUSE Linux Enterprise Software Development Kit 11 for x86-64  
SUSE Linux Enterprise Software Development Kit 11 for x86  
SUSE Linux Enterprise Software Development Kit 11 for s390x  
SUSE Linux Enterprise Software Development Kit 11 for ppc

SUSE Linux Enterprise Software Development Kit 11 for ia64  
SUSE Linux Enterprise Software Development Kit 10 SP3 for x86-64  
SUSE Linux Enterprise Software Development Kit 10 SP3 for x86  
SUSE Linux Enterprise Software Development Kit 10 SP3 for s390x  
SUSE Linux Enterprise Software Development Kit 10 SP3 for ppc  
SUSE Linux Enterprise Software Development Kit 10 SP3 for ia64

TeX:

SUSE Linux Enterprise Desktop 11 for x86-64  
SUSE Linux Enterprise Desktop 11 for x86  
SUSE Linux Enterprise Desktop 10 SP3 for x86-64  
SUSE Linux Enterprise Desktop 10 SP3 for x86  
SUSE Linux Enterprise Software Development Kit 11 for x86-64  
SUSE Linux Enterprise Software Development Kit 11 for x86  
SUSE Linux Enterprise Software Development Kit 11 for s390x  
SUSE Linux Enterprise Software Development Kit 11 for ppc  
SUSE Linux Enterprise Software Development Kit 11 for ia64  
SUSE Linux Enterprise Software Development Kit 10 SP3 for x86-64  
SUSE Linux Enterprise Software Development Kit 10 SP3 for x86  
SUSE Linux Enterprise Software Development Kit 10 SP3 for s390x  
SUSE Linux Enterprise Software Development Kit 10 SP3 for ppc  
SUSE Linux Enterprise Software Development Kit 10 SP3 for ia64

lwlagn-2-6-27-kmp-default:

SUSE Linux Enterprise Desktop 11 for x86-64  
SUSE Linux Enterprise Desktop 11 for x86

Memcached:

SUSE Linux Enterprise Software Development Kit 11 for x86-64  
SUSE Linux Enterprise Software Development Kit 11 for x86  
SUSE Linux Enterprise Software Development Kit 11 for s390x  
SUSE Linux Enterprise Software Development Kit 11 for ppc  
SUSE Linux Enterprise Software Development Kit 11 for ia64  
SUSE Studio Onsite 1.0 [Appliance - Studio] for x86-64

### Notas:

Los servidores OES Linux sólo deben actualizarse siguiendo las instrucciones especificadas en la documentación:

OES 1: Ver "Patching an OES Linux Server" en:

[http://www.novell.com/documentation/oes/install\\_linux/data/bxlu3xc.html](http://www.novell.com/documentation/oes/install_linux/data/bxlu3xc.html)

[http://www.novell.com/documentation/oes2/inst\\_oes\\_lx/data/bxlu3xc.html](http://www.novell.com/documentation/oes2/inst_oes_lx/data/bxlu3xc.html) .

### Referencias en la web:

[http://www.novell.com/documentation/oes/install\\_linux/data/bxlu3xc.html](http://www.novell.com/documentation/oes/install_linux/data/bxlu3xc.html)

[http://www.novell.com/documentation/oes2/inst\\_oes\\_lx/data/bxlu3xc.htm](http://www.novell.com/documentation/oes2/inst_oes_lx/data/bxlu3xc.htm)

### CVEs:

## **Aplicaciones Usuario - Vulnerabilidad en squidguard**

**Fecha:** 5/2/2010

### **Descripción:**

Se ha descubierto una vulnerabilidad en squidguard que podría permitir:

-Un ataque de Denegación de Servicio realizando peticiones de URLs muy largas, y con muchos slashes. Esto provocaría ue el demonio entrase en modo emergencia, con lo que no procesaría más peticiones.

-Saltarse reglas realizando peticiones de URLs cuya longitud está próxima al límite establecido en el buffer.

### **Productos Afectados:**

Debian GNU/Linux 5.0 (lenny/sid)

### **Notas:**

Para la distribución lenny, actualizar el programa a la versión 1.2.0-8.4+lenny1

Para la distribución sid, actualizar el programa a la versión 1.2.0-9

### **Referencias en la web:**

<http://www.debian.org/security/2010/dsa-2040>

### **CVEs:**

CVE-2009-3700, CVE-2009-3826

## Sistemas Operativos - Vulnerabilidad en iscitarget

Fecha: 5/5/2010

### Descripción:

Se han descubierto varias vulnerabilidades en el programa Linux SCSI target framework, permitiendo a los atacantes remotos causar una denegación de servicio en el demonio ietd. La vulnerabilidad podría explotarse enviando una petición modificada de iSNS.

### Productos Afectados:

Debian GNU/Linux 5.0 (lenny)

### Notas:

Para la distribución lenny, los problemas se solucionan al actualizar a la versión 0.4.16+svn162-3.1+lenny1

Para la versión squeeze, los problemas se solucionan al actualizar a la versión: 0.4.17+svn229-1.4.

Para la distribución sid, los problemas se solucionan al actualizar a la versión 0.4.17+svn229-1.4.

### Referencias en la web:

<http://www.debian.org/security/2010/dsa-2042>

### CVEs:

CVE-2010-0743

## **Aplicaciones Usuario - Desbordamiento de enteros en vlc**

**Fecha:** 5/11/2010

### **Descripción:**

Se ha descubierto una vulnerabilidad en vlc debida a la ausencia de validación en la implementación de transporte de datos (RDT), lo que podría permitir un desbordamiento de cálculo entero. Un stream especialmente diseñado podría permitir a un atacante la ejecución de código arbitrario.

### **Productos Afectados:**

Debian GNU/Linux 5.0 (lenny/squeeze)

### **Notas:**

Para la distribución lenny, el problema se soluciona en la versión 0.8.6.h-4+lenny2.3.

Para la distribución squeeze, el problema se soluciona en la versión 1.0.1-1.

### **Referencias en la web:**

<http://www.debian.org/security/2010/dsa-2043>

<http://www.debian.org/security/2010/dsa-2044>

### **CVEs:**

## **Aplicaciones Usuario - Desbordamiento de enteros en libtheora**

**Fecha:** 5/11/2010

### **Descripción:**

Se han encontrado varias vulnerabilidades que podrían permitir a los atacantes, mediante un archivo especialmente diseñado, causar una Denegación de Servicio, e incluso realizar una inyección de código.

### **Productos Afectados:**

Debian GNU/Linux 5.0 (lenny/sid/squeeze)

### **Notas:**

Para la distribución lenny, este problema se ha solucionado en la versión 1.0~beta3-1+lenny1.

Para la distribución squeeze/sid, este problema se ha solventado en la versión 1.1.0-1.

### **Referencias en la web:**

<http://www.debian.org/security/2010/dsa-2045>

### **CVEs:**

CVE-2009-3389

## Servicios (ftp, www, dns, etc.) - Vulnerabilidad en phpgroupware

Fecha: 5/13/2010

### Descripción:

Se han descubierto varias vulnerabilidades en phpgroupware:

-Una vulnerabilidad en la inclusión de un fichero local podría permitir a los atacantes ejecutar código arbitrario e incluir ficheros locales aleatorios.

-Se han encontrado varias vulnerabilidades de SQL injection que permiten la ejecución de sentencias SQL arbitrarias.

### Productos Afectados:

Debian GNU/Linux 5.0 (lenny/squeeze/sid)

### Notas:

Para la distribución lenny, estos problemas se han solventado en la versión 1:0.9.16.012+dfsg-8+lenny2

Para la distribución squeeze y sid, estos problemas se solventarán pronto.

### Referencias en la web:

<http://www.debian.org/security/2010/dsa-2046>

### CVEs:

CVE-2010-0403, CVE-2010-0404

