

BOLETÍN DE VULNERABILIDADES
ÁUDEA, SEGURIDAD DE LA INFORMACIÓN
30 DE ABRIL 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 - 6729779 /Sun Microsystems - 4/23/2010 - Fallo en los tests de fuentes de alimentación redundantes en los equipos SPARC Enterprise M3000/M4000/M5000**
- **Servicios (ftp, www, dns, etc.) - 6902912 /Sun Microsystems - 4/29/2010 - Vulnerabilidad de seguridad en el Software BIND DNS**
- **Sistemas Operativos - 6902220, 6877035 /Sun Microsystems - 4/21/2010 - Fallos en el arranque al actualizar Zpool**
- **Aplicaciones Usuario - 6877323 /Sun Microsystems - 4/21/2010 - Varias Vulnerabilidades de buffer overflow en FreeType 2**
- **Sistemas Operativos - 6745161, 6755267, 6813939 /Sun Microsystems - 4/21/2010 - Vulnerabilidad de Seguridad en la librería libpng de Solaris**
- **Bases de Datos - 6945371 /Sun Microsystems - 4/29/2010 - Pérdida de datos en HIPER-Oracle StorageTek Virtual Tape Control System (VTCS)**
- **Aplicaciones Usuario - 6859039 /Sun Microsystems - 4/21/2010 - Vulnerabilidad de Seguridad en Solaris XScreenSaver**
- **Aplicaciones Usuario - SUSE-SA:2010:022 - 4/21/2010 - Vulnerabilidad de seguridad en Adobe Acrobat Reader**
- **Aplicaciones Usuario - RHSA-2010:0356-02 - 4/19/2010 - Actualización de seguridad en java-1.6.0**
- **Aplicaciones Usuario - RHSA-2010:0361-01 - 4/20/2010 - Actualización de seguridad en "sudo"**
- **Sistemas Operativos - RHSA-2010:0362-01 - 4/20/2010 - Actualización de seguridad en scsi-target-utils**
- **Sistemas Operativos - RHSA-2010:0380-01 - 4/27/2010 - Actualización de seguridad del Kernel**
- **Sistemas Operativos - RHSA-2010:0382-01 - 4/28/2010 - Actualización de seguridad en xorg-x11-server**
- **Aplicaciones Usuario - RHSA-2010:0383-01 - 4/29/2010 - Actualización de Seguridad en: java-1.6.0-ibm**
- **Servicios (ftp, www, dns, etc.) - VUPEN/ADV-2010-0995 - 4/27/2010 - Apache Tomcat Web Application Manager / Host Manager Vulnerability**

2. Boletín Detallado Vulnerabilidades

Sistemas Operativos - Fallo en los tests de fuentes de alimentación redundantes en los equipos SPARC Enterprise M3000/M4000/M5000

Fecha: 4/23/2010

Descripción:

Los Servidores SPARC Enterprise M3000/M4000/M5000 que ejecutan una versión del firmware anterior a la 1090 se ven afectados por un error a la hora de verificar la redundancia de la fuente de alimentación, dando como resultado fallos en el arranque.

Además, ciertos componentes informarán de ciertos errores, aunque estos no sean ciertos, impulsando la necesidad de reemplazar los componentes por otros nuevos.

Productos Afectados:

Sun SPARC Enterprise M4000 Server

Sun SPARC Enterprise M5000 Server

Sun SPARC Enterprise M3000 Server

Notas:

Solución:

Instalar el nuevo firmware desde la URL:

https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/CDS-CDS_SMI-Site/en_US/-/USD/ViewProductDetail-Start?ProductRef=OPL-M3-4-5-8-9000-XCP-1090-SP-G-F@CDS-CDS_SMI

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-269808-1>

https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/CDS-CDS_SMI-Site/en_US/-/USD/ViewProductDetail-Start?ProductRef=OPL-M3-4-5-8-9000-XCP-1090-SP-G-F@CDS-CDS_SMI

CVEs:

Servicios (ftp, www, dns, etc.) - Vulnerabilidad de seguridad en el Software BIND DNS

Fecha: 4/29/2010

Descripción:

Una vulnerabilidad de seguridad en el programa BIND DNS de Solaris podría permitir a un usuario remoto capaz de realizar consultas recursivas causar un comportamiento anómalo en el servidor, devolviendo direcciones incorrectas para los hosts de Internet. Esto permitiría redirigir a los usuarios a servicios y hosts de dudosa confianza.

Productos Afectados:

SPARC Platform

Solaris 9 without patch 112837-21

Solaris 10 without patch 119783-14

OpenSolaris based upon builds snv_01 through snv_130

x86 Platform

Solaris 9 without patch 114265-20

Solaris 10 without patch 119784-14

OpenSolaris based upon builds snv_01 through snv_130

Notas:

Solución:

Instalar los siguientes parches:

SPARC Platform

Solaris 9 with patch 112837-21 or later

Solaris 10 with patch 119783-14 or later

OpenSolaris based upon builds snv_131 or later

x86 Platform

Solaris 9 with patch 114265-20 or later

Solaris 10 with patch 119784-14 or later

OpenSolaris based upon builds snv_131 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-273169-1>

CVEs:

Sistemas Operativos - Fallos en el arranque al actualizar Zpool

Fecha: 4/21/2010

Descripción:

El parche 141445 para la plataforma Solaris 10 x86 ofrece soporte para una nueva versión de zpool. Esta nueva versión tiene dos vulnerabilidades potenciales en los sistemas con un fichero de sistema root ZFS, que podría provocar un error en el arranque. Además de este problema, se produce un fallo en la actualización del kernel al actualizar GRUB, y el sistema de ficheros seguro.

La instalación del parche 141445-09 no tendrá ningún impacto negativo de forma inicial. No obstante, al actualizar de forma posterior la versión de ZFS root pool mediante la aplicación "zpool upgrade rpool" se generarán los siguientes problemas:

-El sistema no será capaz tras reiniciarse

Nos nuevos entornos (Bes) creados después de la actualización

Productos Afectados:

Solaris 8

Solaris 9

Opensolaris

Notas:

La solución al problema aún está pendiente de publicación.

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-276010-1>

CVEs:

Aplicaciones Usuario - Varias Vulnerabilidades de buffer overflow en FreeType 2

Fecha: 4/21/2010

Descripción:

Se han encontrado varias vulnerabilidades de Buffer Overflow en la librería de fuentes de Free Type 2, lo que podría afectar de forma negativa a las aplicaciones que utilizan esta librería. Dependiendo de la aplicación, esta vulnerabilidad podría permitir a un usuario local o remoto sin privilegios bloquear la aplicación a través de un archivo de fuentes especialmente diseñado, resultando en una Denegación de Servicio, o en la ejecución de código arbitrario con los privilegios del usuario que ejecuta la aplicación.

Productos Afectados:

SPARC Platform

X11 6.4.1 (for Solaris 8)

Solaris 9

Solaris 10 without patch 119812-07

OpenSolaris based upon builds snv_01 through snv_123

x86 Platform

X11 6.4.1 (for Solaris 8)

Solaris 9

Solaris 10 without patch 119813-09

OpenSolaris based upon builds snv_01 through snv_123

Notas:

Solución:

Instalar los siguientes parches:

SPARC Platform

Solaris 10 with patch 119812-07 or later

OpenSolaris based upon builds snv_124 or later

x86 Platform

Solaris 10 with patch 119813-09 or later

OpenSolaris based upon builds snv_124 or later

Referencias en la web:

Sistemas Operativos - Vulnerabilidad de Seguridad en la librería libpng de Solaris

Fecha: 4/21/2010

Descripción:

Se han encontrado varias vulnerabilidades en la librería libpng incluida en Solaris, que podrían permitir a un usuario remoto sin privilegios causar una Denegación de Servicio en aplicaciones enlazadas a libpng, o potencialmente ejecutar código arbitrario con privilegios del usuario que ejecuta la aplicación, cuando un usuario a cargado un archivo de imagen PNG especialmente diseñado.

Productos Afectados:

SPARC Platform

GNOME 2.0 (for Solaris 8)

Solaris 9

Solaris 10 without patch 137080-03

OpenSolaris builds snv_01 through snv_112

x86 Platform

GNOME 2.0 (for Solaris 8)

Solaris 9

Solaris 10 without patch 137081-03

OpenSolaris builds snv_01 through snv_112

Notas:

Solución: Instalar los siguientes parches:

SPARC Platform

Solaris 10 with patch 137080-03 or later

OpenSolaris based upon builds snv_113 or later

x86 Platform

Solaris 10 with patch 137081-03 or later

OpenSolaris based upon builds snv_113 or later

Referencias en la web:

Bases de Datos - Pérdida de datos en HIPER-Oracle StorageTek Virtual Tape Control System (VTCS)

Fecha: 4/29/2010

Descripción:

El producto Oracle StorageTek Virtual Tape Control System (VTCS) podría experimentar una pérdida de datos en una situación de recuperación CDS porque el comando LOGUTIL/GENAUDIT podría completarse de forma prematura con una condición igual a cero.

Productos Afectados:

Oracle StorageTek ELS 7.0 with PTF L1H15J8 (patch 135437-01)

Notas:

Solución: Está pendiente de publicarse un parche que solucione el problema.

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-279850-1>

CVEs:

Aplicaciones Usuario - Vulnerabilidad de Seguridad en Solaris XScreenSaver

Fecha: 4/21/2010

Descripción:

Se ha encontrado una vulnerabilidad de seguridad en el programa Solaris XScreenSaver que podría permitir a un usuario local sin privilegios leer información sensible.

Productos Afectados:

SPARC PlatformGNOME 2.0 (Solaris 8)

GNOME 2.0 (Solaris 9)

GNOME 2.0.2 (Solaris 9)

Solaris 10 without patch 120094-26

OpenSolaris based upon builds snv_01 through snv_120

x86 PlatformGNOME 2.0 (Solaris 8)

GNOME 2.0 (Solaris 9)

GNOME 2.0.2 (Solaris 9)

Solaris 10 without patch 120095-26

OpenSolaris based upon builds snv_01 through snv_120

Notas:

Solución: Instalar los siguientes parches:

SPARC PlatformSolaris 10 with patch 120094-26 or later

OpenSolaris based upon builds snv_121 or later

x86 PlatformSolaris 10 with patch 120095-26 or later

OpenSolaris based upon builds snv_121 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-264048-1>

CVEs:

Aplicaciones Usuario - Vulnerabilidad de seguridad en Adobe Acrobat Reader

Fecha: 4/21/2010

Descripción:

Se ha descubierto una vulnerabilidad en Adobe Acrobat Reader que podría provocar que el programa dejase de funcionar, o que un atacante ejecutase código arbitrario.

Productos Afectados:

openSUSE 11.0

openSUSE 11.1

openSUSE 11.2

SUSE Linux Enterprise Desktop 10 SP2

SUSE Linux Enterprise Desktop 10 SP3

SUSE Linux Enterprise Desktop 11

Notas:

Solución:

Instalar todas las actualizaciones relacionadas con acroread, reinicializar todas las instancias al completar la instalación.

Más información y descargas en:

http://www.novell.com/linux/security/advisories/2010_22_acroread.html

Referencias en la web:

http://www.novell.com/linux/security/advisories/2010_22_acroread.html

CVEs:

CVE-2010-0190, CVE-2010-0191, CVE-2010-0192, CVE-2010-0193, CVE-2010-0194, CVE-2010-0195, CVE-2010-0196, CVE-2010-0197, CVE-2010-0198, CVE-2010-0199, CVE-2010-0201, CVE-2010-0202, CVE-2010-0203, CVE-2010-0204, CVE-2010-1241

Aplicaciones Usuario - Actualización de seguridad en java-1.6.0

Fecha: 4/19/2010

Descripción:

Se han actualizado los paquetes de java-1.6.0-sun que solucionan dos problemas de seguridad que afectaban a Java Runtime Environment y al Software Development Kit.

Las instancias de Java deberán reiniciarse tras completar la actualización

Productos Afectados:

RHEL Desktop Supplementary (v. 5 client) - i386, x86_64 RHEL Supplementary (v. 5 server) - i386, x86_64
Red Hat Desktop version 4 Extras - i386, x86_64 Red Hat Enterprise Linux AS version 4 Extras - i386, x86_64
Red Hat Enterprise Linux ES version 4 Extras - i386, x86_64 Red Hat Enterprise Linux WS version 4 Extras - i386, x86_64

Notas:

Se puede obtener más información sobre la instalación del parche en:

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

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0356.html>

CVEs:

CVE-2010-0886 CVE-2010-0887

Aplicaciones Usuario - Actualización de seguridad en "sudo"

Fecha: 4/20/2010

Descripción:

Se añadió la capacidad de poder cambiar el valor de la opción `ignore_dot` del fichero de configuración `/etc/sudoers`. En las configuraciones en las que la opción `ignore_dot` se establece a `off` (es el valor que trae por defecto), un usuario local autorizado a utilizar el comando `sudedit` odría ejecutar comandos arbitrarios con más permisos de los que le corresponden.

Productos Afectados:

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:

Solución: Descargar e instalar el parche. Se puede obtener más información sobre la 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-2010-0361.html>

CVEs:

CVE-2010-1163

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

Fecha: 4/20/2010

Descripción:

Existe un problema en el formato de cadenas de caracteres en el demonio tgtd. Un atacante remoto podría aprovechar esta vulnerabilidad para enviar un iSNS (Internet Storage Name Service) especialmente diseñado, causando que el demonio tgtd deje de funcionar.

Productos Afectados:

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

Notas:

Para solventar el problema es necesario instalar la actualización.

Se puede obtener información sobre la instalación 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-2010-0362.html>

CVEs:

CVE-2010-0743

Sistemas Operativos - Actualización de seguridad del Kernel

Fecha: 4/27/2010

Descripción:

Se han solventado las siguientes vulnerabilidades:

-Se ha encontrado una condición "race" en la implementación de MAC80211, que es un framework utilizado para diseñar drivers wireless.

Un atacante podría aprovechar esta vulnerabilidad enviando un paquete Delete Block ACK (DELBA) al equipo objetivo, provocando una Denegación de Servicio.

-Se ha encontrado una vulnerabilidad en la función tcp_rcv_state_process() del protocolo TCP/IP del kernel. Si un sistema que utiliza IPv6 tiene la opción IPV6_RECVPKTINFO establecida en un socket en estado "listening", un atacante podría enviar un paquete malicioso que causara un "Kernel Panic" (Denegación de Servicio).

-Se ha encontrado un problema en la implementación de gfs2_lock(). EL locking code GFS2 podría saltarse la operación de "lock" en los ficheros que tienen el bit S_ISGID establecido.

Un usuario local sin privilegios podría utilizar este problema para causar un Kernel Panic (Denegación de Servicio).

-Se ha encontrado un problema en el sistema de ficheros EXT 4 que podría permitir realizar una división entre 0. Un atacante podría utilizar este problema para provocar una denegación de servicio.

Productos Afectados:

Red Hat Enterprise Linux (v. 5.4.z server) - i386, ia64, noarch, ppc, s390x, x86_64

Notas:

Se puede encontrar información sobre los parches a instalar en:

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

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0380.html>

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

CVEs:

CVE-2009-4027 CVE-2009-4307 CVE-2010-0727 CVE-2010-1188

Sistemas Operativos - Actualización de seguridad en xorg-x11-server

Fecha: 4/28/2010

Descripción:

Se ha descubierto un error de cálculo en la extensión Xorg Render.

Un cliente malicioso y no autorizado podría explotar esta vulnerabilidad para parar el servicio o , incluso, ejecutar código arbitrario.

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 información sobre el parche a instalar 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-2010-0382.html>

CVEs:

CVE-2010-1166

Aplicaciones Usuario - Actualización de Seguridad en: java-1.6.0-ibm

Fecha: 4/29/2010

Descripción:

LA actualización soluciona varias vulnerabilidades en Java 2 Runtime Environment y IBM Java 2 Software Development Kit. Estas vulnerabilidades están englobadas en la página IBM "Security alerts". (CVE-2010-0084, CVE-2010-0085, CVE-2010-0087, CVE-2010-0088, CVE-2010-0089, CVE-2010-0090, CVE-2010-0091, CVE-2010-0092, CVE-2010-0094, CVE-2010-0095, CVE-2010-0837, CVE-2010-0838, CVE-2010-0839, CVE-2010-0840, CVE-2010-0841, CVE-2010-0842, CVE-2010-0843, CVE-2010-0844, CVE-2010-0846, CVE-2010-0848, CVE-2010-0849)

Productos Afectados:

RHEL Desktop Supplementary (v. 5 client) - i386, x86_64 RHEL Supplementary (v. 5 server) - i386, ppc, s390x, x86_64 Red Hat Desktop version 4 Extras - i386, x86_64 Red Hat Enterprise Linux AS version 4 Extras - i386, ppc, s390, s390x, x86_64 Red Hat Enterprise Linux ES version 4 Extras - i386, x86_64 Red Hat Enterprise Linux WS version 4 Extras - i386, x86_64

Notas:

Se puede encontrar información sobre los parches a instalar en:

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

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0383.html>

CVEs:

CVE-2010-0084 CVE-2010-0085 CVE-2010-0087 CVE-2010-0088 CVE-2010-0089 CVE-2010-0090 CVE-2010-0091 CVE-2010-0092 CVE-2010-0094 CVE-2010-0095 CVE-2010-0837 CVE-2010-0838 CVE-2010-0839 CVE-2010-0840 CVE-2010-0841 CVE-2010-0842 CVE-2010-0843 CVE-2010-0844 CVE-2010-0846 CVE-2010-0848 CVE-2010-0849

Servicios (ftp, www, dns, etc.) - Apache Tomcat Web Application Manager / Host Manager Vulnerability

Fecha: 4/27/2010

Descripción:

Existe una vulnerabilidad en Apache Tomcat, que puede ser explotada para llevar a cabo un ataque cross-site. El error se debe problemas en la validación en los componentes Web Application Manager y Host Manager al procesar peticiones HTTP, que podrían ser explotadas por un atacante para manipular información.

Productos Afectados:

Apache Tomcat versions 6.x

Apache Tomcat versions 5.x

Notas:

Referencias en la web:

<http://www.vupen.com/english/advisories/2010/0995>

CVEs:

Calle Playa de Liencres, 2
EUROPA EMPRESARIAL Edif Londres Bajo-6
Teléfono: 91 745 11 57
Fax: 91 636 63 96
28230 Las Rozas - Madrid



www.audea.com
info@audea.com