

BOLETÍN DE VULNERABILIDADES
ÁUDEA, SEGURIDAD DE LA INFORMACIÓN
31 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 - SUSE-SA:2010:031 - 7/20/2010 - Actualizaciones de seguridad en el Kernel de SUSE Linux**
- **Aplicaciones Usuario - SUSE-SA:2010:032 - 7/30/2010 - Actualizaciones de Mozilla Firefox, Thunderbird y Seamonkey**
- **Aplicaciones Usuario - RHSA-2010:0549-01 - 7/21/2010 - Actualizaciones de seguridad en componentes de java para Red Hat Linux**
- **Servicios (ftp, www, dns, etc.) - RHSA-2010:0556-01 - 7/23/2010 - Actualización de seguridad en Firefox para Red Hat**
- **Servicios (ftp, www, dns, etc.) - RHSA-2010:0557-01 - 7/23/2010 - Actualizaciones de seguridad en Seamonkey**
- **Sistemas Operativos - RHSA-2010:0565-01 - 7/27/2010 - Actualización w3m**
- **Sistemas Operativos - RHSA-2010:0567-01 - 7/28/2010 - Actualización de seguridad en lvm2 cluster**
- **Aplicaciones Usuario - RHSA-2010:0574-01 - 7/29/2010 - Actualización de: java-1.4.2-ibm**
- **Sistemas Operativos - RHSA-2010:0576-01 - 7/30/2010 - Notificaciones End of Life Plans de productos Red Hat**
- **Aplicaciones Usuario - RHSA-2010:0577-01 - 7/30/2010 - Actualización de seguridad en freetype**
- **Aplicaciones Usuario - HT4263 /Apple - 7/21/2010 - Vulnerabilidades de Seguridad en iTunes 9.2.1**
- **Servicios (ftp, www, dns, etc.) - HT4276 /Apple - 7/28/2010 - Actualizaciones de Seguridad en Safari 5.0.1 y Safari 4.1.1**

2. Boletín Detallado Vulnerabilidades

Sistemas Operativos - Actualizaciones de seguridad en el Kernel de SUSE Linux

Fecha: 7/20/2010

Descripción:

Se han publicado varios paquetes de actualización del kernel que solucionan las siguientes vulnerabilidades:

-La función `do_gfs2_set_flags` del kernel de linux presente en `fs/gfs2/file.c` no verifica el propietario del fichero, lo que podría permitir a usuarios locales saltarse restricciones de acceso mediante peticiones `SETFLAGS ioctl`.

-La función `nfs_wait_on_request` del kernel de linux presente en `fs/nfs/pagelist.c` permite a los atacantes causar una denegación de servicio mediante vectores de ataque desconocidos, para conseguir "truncar" un fichero e intrumpir una operación que es ininterrumpible.

-Cuando la opción "overcommit" está habilitada en el fichero `mm/shmem.c`, los objetos `shmemfs` no se exportan correctamente con `knfsd`, lo que podría permitir a los atacantes causar una denegación de servicio (referencia a `NULL` y bloqueo de `knfsd`).

Productos Afectados:

SUSE Linux Enterprise High Availability Extension 11

SUSE Linux Enterprise Desktop 11

SUSE Linux Enterprise Server 11

Notas:

Se puede encontrar mas información sobre los problemas solventados en:

http://www.novell.com/linux/security/advisories/2010_31_kernel.html

Referencias en la web:

http://www.novell.com/linux/security/advisories/2010_31_kernel.html

CVEs:

CVE-2009-1389, CVE-2009-4537, CVE-2010-1087, CVE-2010-1162, CVE-2010-1437, CVE-2010-1446, CVE-2010-1641, CVE-2010-1643

Aplicaciones Usuario - Actualizaciones de Mozilla Firefox, Thunderbird y Seamonkey

Fecha: 7/30/2010

Descripción:

Se han publicado varias actualizaciones de seguridad que solucionan problemas de seguridad diversos en los productos Mozilla Firefox, Mozilla Thunderbird y Seamonkey.

Productos Afectados:

openSUSE 11.1
openSUSE 11.2
openSUSE 11.3
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
SUSE Linux Enterprise Software Development Kit 11 SP1
SUSE Linux Enterprise Desktop 11 SP1
SUSE Linux Enterprise Server 11 SP1

Notas:

Se puede encontrar información sobre los problemas resueltos en las actualizaciones vistando el siguiente enlace:

http://www.novell.com/linux/security/advisories/2010_32_mozilla.html

Referencias en la web:

http://www.novell.com/linux/security/advisories/2010_32_mozilla.html

CVEs:

CVE-2010-0654, CVE-2010-1205, CVE-2010-1206, CVE-2010-1207, CVE-2010-1208, CVE-2010-1209, CVE-2010-1210, CVE-2010-1211, CVE-2010-1212, CVE-2010-1213, CVE-2010-1214, CVE-2010-1215, CVE-2010-2751, CVE-2010-2752, CVE-2010-2753, CVE-2010-2754, CVE-2010-2755, MFSA 2010-34, MFSA 2010-35, MFSA 2010-36, MFSA 2010-37, MFSA 2010-38, MFSA 2010-39, MFSA 2010-40, MFSA 2010-41, MFSA 2010-42, MFSA 2010-43, MFSA 2010-44, MFSA 2010-45, MFSA 2010-46, MFSA 2010-47, MFSA 2010-48, MFSA 2011-42

Aplicaciones Usuario - Actualizaciones de seguridad en componentes de java para Red Hat Linux

Fecha: 7/21/2010

Descripción:

Se han actualizado los paquetes java-1.6.0-ibm que solucionan un problema de seguridad en Red Hat Enterprise Linux 4 Extras y 5 Supplementary.

Esta vulnerabilidad se ha categorizado como crítica, por lo que se recomienda instalar las actualizaciones lo antes posible.

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 más información sobre las actualizaciones y los problemas que resuelven en:

<https://rhn.redhat.com/errata/RHSA-2010-0549.html>

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0549.html>

CVEs:

CVE-2010-0887

Servicios (ftp, www, dns, etc.) - Actualización de seguridad en Firefox para Red Hat

Fecha: 7/23/2010

Descripción:

Se han publicado paquetes actualizados de xulrunner que solucionan un problema de seguridad en Red Hat Enterprise Linux 5.

El error se encuentra en plugin handler de firefox. U nataque con contenido web malicioso podría provocar un puntero que apunta a una dirección de memoria errónea, cuasando el bloqueo de firefox, o ejecutar código arbitrario con los privilegios del usuario que ejecuta la aplicación Firefox.

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 los problemas solventados en la actualización descrita, visitando el siguiente enlace:

<https://rhn.redhat.com/errata/RHSA-2010-0556.html>

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0556.html>

CVEs:

CVE-2010-2755

Servicios (ftp, www, dns, etc.) - Actualizaciones de seguridad en Seamonkey

Fecha: 7/23/2010

Descripción:

Se han publicado actualizaciones de seamonkey que solucionan un problema de seguridad. Dicho problema se encuentra en el plugin handler. Realizando un ataque mediante contenido web malicioso se podría provocar que un puntero apuntase a una posición errónea de memoria, causando un bloqueo de SeaMonkey o ejecutar código arbitrario con los privilegios del usuario que ejecuta SeaMonkey. Todos los usuarios de Seamonkey debería instalar estas actualizaciones.

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 AS version 4 - i386, ia64, ppc, s390, s390x, 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 las actualizaciones descritas en:
<https://rhn.redhat.com/errata/RHSA-2010-0557.html>

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0557.html>

CVEs:

CVE-2010-2755

Sistemas Operativos - Actualización w3m

Fecha: 7/27/2010

Descripción:

Se han actualizado los paquetes de w3m que que solventan un problema de seguridad en Red Hat Enterprise Linux 5.

Se ha descubierto que w3m está afectada por una vulnerabilidad previamente publicada, conocida como: "null prefix attack", causada por el tratamiento incorrecto de los caracteres nulos en los certificados X509. Si un atacante es capaz de obtener un certificado especialmente diseñado, firmado por una Entidad Certificadora de confianza el atacante podría utilizar el certificado durante un ataque de tipo Man in The Middle, e incluso provocar que w3m acepte el certificado.

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:

Se puede encontrar más información sobre las actualizaciones publicadas en:

<https://rhn.redhat.com/errata/RHSA-2010-0565.html>

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0565.html>

CVEs:

CVE-2010-2074

Sistemas Operativos - Actualización de seguridad en lvm2 cluster

Fecha: 7/28/2010

Descripción:

Se ha descubierto que el demonio del Administrador de volúmenes de clusters lógicos no verifica las credenciales de los clientes que se conectan al socket de control de abstracción de UNIX, permitiendo a los usuarios locales no autenticados enviar comandos de control que sólo estaban disponibles para el usuario maestro root. Esto podría provocar que un usuario sin privilegios cause un clvmd para salir o una petición clvmd para activar, desactivar o recargar cualquier volumen lógico del sistema local, o de otro sistema del cluster.

Productos Afectados:

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

Notas:

Se puede más información sobre la actualización en:

<https://rhn.redhat.com/errata/RHSA-2010-0567.html>

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0567.html>

CVEs:

CVE-2010-2526

Aplicaciones Usuario - Actualización de: java-1.4.2-ibm

Fecha: 7/29/2010

Descripción:

Se han actualizado los paquetes de java-1.4.2-ibm que solucionan varios problemas de seguridad en Red Hat Linux 3-4 Extras, y Red Hat Enterprise Linux Supplementary.

Productos Afectados:

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

RHEL Supplementary (v. 5 server) - i386, ia64, ppc, s390x, x86_64

Red Hat Desktop version 3 Extras - i386, x86_64

Red Hat Desktop version 4 Extras - i386, x86_64

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

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

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

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

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

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

Notas:

Se puede encontrar más información sobre las actualizaciones citadas en:

<https://rhn.redhat.com/errata/RHSA-2010-0574.html>

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0574.html>

CVEs:

CVE-2010-0084 CVE-2010-0085 CVE-2010-0087 CVE-2010-0088 CVE-2010-0089 CVE-2010-0091 CVE-2010-0095 CVE-2010-0839 CVE-2010-0840 CVE-2010-0841 CVE-2010-0842 CVE-2010-0843 CVE-2010-0844 CVE-2010-0846 CVE-2010-0847 CVE-2010-0848 CVE-2010-0849

Sistemas Operativos - Notificaciones End of Life Plans de productos Red Hat

Fecha: 7/30/2010

Descripción:

El ciclo de vida de 7 años del producto Red Hat Enterprise Linux 3 finalizará el 31 de Octubre del 2010. Después de esta fecha, Red Hat discontinuará los servicios de suscripción para Red Hat 3. No se publicarán parches de seguridad y actualizaciones que solucionen problemas del sistema.

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 Red Hat Enterprise Linux versión 5.

Se puede encontrar más información en:

<https://rhn.redhat.com/errata/RHSA-2010-0576.html>

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0576.html>

CVEs:

Aplicaciones Usuario - Actualización de seguridad en freetype

Fecha: 7/30/2010

Descripción:

Se ha publicado una actualización que soluciona una vulnerabilidad de buffer overflow producida por la forma el motor de fuentes procesa ficheros de fuentes.. Si un usuario carga un fichero de fuentes especialmente diseñado con una aplicación que utiliza freetype, podría causar que la aplicación deje de funcionar o, pueda permitir la ejecución de código arbitrario con privilegios del usuario que ejecuta la aplicación.

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 puede encontrar más información sobre la actualización en el siguiente enlace:

<https://rhn.redhat.com/errata/RHSA-2010-0577.html>

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0577.html>

CVEs:

CVE-2010-2500 CVE-2010-2527 CVE-2010-2541

Aplicaciones Usuario - Vulnerabilidades de Seguridad en Itunes 9.2.1

Fecha: 7/21/2010

Descripción:

la visita a un sitio web creado con fines malintencionados puede ocasionar la finalización inesperada de la aplicación o la ejecución de código arbitrario

Descripción: se produce un desbordamiento de búfer en el manejo de las URL "itpc:". El acceso a una URL "itpc:" creada con fines malintencionados puede ocasionar la finalización inesperada de la aplicación o la ejecución de código arbitrario. Este problema se soluciona mejorando la comprobación de los límites. Gracias a Clint Ruoho de Laconic Security por informar de este problema.

Productos Afectados:

Itunes 9.2.1

Notas:

Se puede encontrar más información sobre la actualización en:

http://support.apple.com/kb/HT4263?viewlocale=es_ES

Referencias en la web:

http://support.apple.com/kb/HT4263?viewlocale=es_ES

CVEs:

CVE-2010-1777

Servicios (ftp, www, dns, etc.) - Actualizaciones de Seguridad en Safari 5.0.1 y Safari 4.1.1

Fecha: 7/28/2010

Descripción:

CVE-ID: CVE-2010-1778

Disponible para: Mac OS X v10.4.11, Mac OS X Server v10.4.11, Mac OS X v10.5.8, Mac OS X Server v10.5.8, Mac OS X v10.6.2 o posterior, Mac OS X Server v10.6.2 o posterior, Windows 7, Vista, XP SP2 o posterior

Impacto: el acceso a una fuente RSS creada con fines malintencionados puede provocar que se envíen archivos del sistema del usuario a un servidor remoto

Descripción: Safari presenta un problema de visualización mediante script de páginas web de contenido sospechoso en el manejo de fuentes RSS. El acceso a una fuente RSS creada con fines malintencionados puede provocar que se envíen archivos del sistema del usuario a un servidor remoto. Este problema se trata a través de un manejo mejorado de las fuentes RSS. Gracias a Billy Rios, del equipo de seguridad de Google, por informar de este problema.

CVE-ID: CVE-2010-1796

Disponible para: Mac OS X v10.4.11, Mac OS X Server v10.4.11, Mac OS X v10.5.8, Mac OS X Server v10.5.8, Mac OS X v10.6.2 o posterior, Mac OS X Server v10.6.2 o posterior, Windows 7, Vista, XP SP2 o posterior

Impacto: la función de autorrelleno de Safari podría revelar información a sitios web sin ninguna interacción por parte del usuario

Descripción: la función de autorrelleno de Safari podría rellenar formularios web de forma automática utilizando información contenida en la agenda de Mac OS X, en Outlook o en la agenda de Windows. En condiciones normales es necesaria la intervención del usuario para que Autorrellenar actúe en un formulario web. Existe un problema de implementación que permite a las páginas web creadas con fines maliciosos activar Autorrellenar sin la intervención del usuario. Esto puede provocar que se revele información contenida en la tarjeta de Agenda del usuario. Para que este problema se produzca, es necesario que se den las dos condiciones que se describen a continuación. En primer lugar, en las preferencias de Safari, en Autorrelleno, la casilla de verificación "Autorrellenar formularios web con la información de la tarjeta de mi Agenda" debe estar seleccionada. La segunda condición es que la agenda del usuario debe contar con una tarjeta designada como "Mi tarjeta". Autorrellenar sólo accede a la información de esa tarjeta en concreto. Este problema se resuelve prohibiendo a Autorrellenar que utilice la información sin la intervención del usuario. No afecta a los dispositivos que ejecuten iOS. Gracias a Jeremiah Grossman, de WhiteHat Security, por informar de este problema.

Productos Afectados:

Safari 5.0.1

Safari 4.1.1

Notas:

Más información sobre las actualizaciones:

http://support.apple.com/kb/HT4276?viewlocale=es_ES

Referencias en la web:

http://support.apple.com/kb/HT4276?viewlocale=es_ES

CVEs:

CVE-2010-1778 CVE-2010-1796

