

BOLETÍN DE VULNERABILIDADES
ÁUDEA, SEGURIDAD DE LA INFORMACIÓN
28 DE FEBRERO DE 2011

[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

- Servicios (ftp, www, dns, etc.) - RHTSA-2011:0256-01 - 2/15/2011 - **Actualización de Seguridad en DHCP**
- Sistemas Operativos - RHTSA-2011:0257-01 - 2/15/2011 - **Actualización de Seguridad en Subversion**
- Sistemas Operativos - RHTSA-2011:0259-01 - 2/15/2011 - **Actualización del plugin de flash**
- Aplicaciones Usuario - RHTSA-2011:0260-01 - 2/16/2011 - **Actualización de seguridad en python**
- Aplicaciones Usuario - RHTSA-2011:0261-01 - 2/16/2011 - **Actualización de seguridad y solución de un bug en bash**
- Servicios (ftp, www, dns, etc.) - RHTSA-2011:0262-01 - 2/16/2011 - **Actualización de seguridad en sendmail**
- Sistemas Operativos - RHTSA-2011:0266-01 - 2/16/2011 - **Actualización de seguridad en Red Hat Cluster Suite 4**
- Sistemas Operativos - RHTSA-2011:0279-01 - 2/16/2011 - **Ampliación del soporte de Red Hat Enterprise Linux 4.7**
- Aplicaciones Usuario - RHTSA-2011:0281-01 - 2/17/2011 - **Actualización de Seguridad en java-1.6.0-openjdk**
- Aplicaciones Usuario - RHTSA-2011:0282-01 - 2/17/2011 - **Actualización de seguridad en Java-1-6-0**
- Sistemas Operativos - DSA-2169-1 - 2/16/2011 - **Validación de entrada insuficiente en telepathy gabble**
- Aplicaciones Usuario - DSA-2170-1 - 2/18/2011 - **Actualizaciones de seguridad en mailman**
- Aplicaciones Usuario - DSA-2171-1 - 2/21/2011 - **Vulnerabilidad de seguridad en Asterisk**
- Aplicaciones Usuario - RHTSA-2011:0292-01 - 2/22/2011 - **Actualización de seguridad en java-1.4.2-ibm**
- Aplicaciones Usuario - RHTSA-2011:0301-01 - 2/23/2011 - **Actualización de Seguridad en Acroread**
-

2. Boletín Detallado Vulnerabilidades

Servicios (ftp, www, dns, etc.) - Actualización de Seguridad en DHCP

Fecha: 2/15/2011

Descripción:

Se ha encontrado un error en la forma en la que el demonio dhcpd procesa ciertos mensajes DHCPv6 para direcciones que han sido declinadas y marcadas como abandonadas de forma interna de forma previa. Si un atacante remoto envía estos mensajes a dhcpd, el servicio podría bloquearse, además de provocarse un fallo de aserción si se ejecutaba en un servidor DHCPV6.

Productos Afectados:

Red Hat Enterprise Linux Desktop (v. 6) - i386, x86_64

Red Hat Enterprise Linux Desktop Optional (v. 6) - i386, x86_64

Red Hat Enterprise Linux HPC Node (v. 6) - x86_64

Red Hat Enterprise Linux HPC Node Optional (v. 6) - x86_64

Red Hat Enterprise Linux Server (v. 6) - i386, ppc64, s390x, x86_64

Red Hat Enterprise Linux Server Optional (v. 6) - i386, ppc64, s390x, x86_64

Red Hat Enterprise Linux Workstation (v. 6) - i386, x86_64

Red Hat Enterprise Linux Workstation Optional (v. 6) - i386, x86_64

Notas:

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

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

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2011-0256.html>

CVEs:

CVE-2011-0413

Sistemas Operativos - Actualización de Seguridad en Subversion

Fecha: 2/15/2011

Descripción:

Se ha encontrado un fallo de fuga de información en memoria en la parte servidor. Si un usuario remoto malicioso realiza operaciones "svn blame" o "svn log" en ciertos ficheros del repositorio, se podría causar un consumo excesivo de memoria del sistema.

Se ha encontrado un referencia inválida a punteros que afecta a la forma en la que mod_dav_svn procesa ciertas peticiones. Si un usuario remoto malicioso solicita un tipo de petición para mostrar una colección de los repositorios de Subversion en un host que tiene la directiva SVNListParentPath activada, se podría causar un bloqueo del proceso httpd.

Productos Afectados:

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

Red Hat Enterprise Linux (v. 5 server) - i386, ia64, ppc, s390x, 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-2011-0257.html>

CVEs:

CVE-2010-4539 CVE-2010-4644

Sistemas Operativos - Actualización del plugin de flash

Fecha: 2/15/2011

Descripción:

El plugin de flash en Red Hat Enterprise Linux 4 tiene varias vulnerabilidades de seguridad y no debería utilizarse. Esta es la primera notificación del mes en la que Red Hat planea deshabilitar Flash Player 9 en Red Hat Enterprise Linux 4.

Productos Afectados:

Red Hat Desktop version 4 Extras - i386

Red Hat Enterprise Linux AS version 4 Extras - i386

Red Hat Enterprise Linux ES version 4 Extras - i386

Red Hat Enterprise Linux WS version 4 Extras - i386

Notas:

Se puede encontrar más información en:

<https://rhn.redhat.com/errata/RHSA-2011-0259.html>

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2011-0259.html>

<https://access.redhat.com/security/updates/classification/#critical>

<http://kb2.adobe.com/cps/406/kb406791.html>

<https://access.redhat.com/kb/docs/DOC-1639>

CVEs:

CVE-2011-0558, CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0575, CVE-2011-0577, CVE-2011-0578, CVE-2011-0607, CVE-2011-0608

Aplicaciones Usuario - Actualización de seguridad en python

Fecha: 2/16/2011

Descripción:

Se han encontrado varias vulnerabilidades en el módulo rgbimg de Python. Si una aplicación escrita en Python utiliza el módulo rgbimg y carga un fichero de imagen SGI especialmente manipulada, se podría causar un bloqueo de la aplicación o , permitir la ejecución de código arbitrario con los privilegios del usuario que ejecuta la aplicación.

Productos Afectados:

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 4 - i386, ia64, x86_64

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

Notas:

Se puede encontrar más información en:

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

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2011-0260.html>

CVEs:

CVE-2009-4134 CVE-2010-1449 CVE-2010-1450

Aplicaciones Usuario - Actualización de seguridad y solución de un bug en bash

Fecha: 2/16/2011

Descripción:

Se ha descubierto que varios scripts incluidos en la documentación de Bash crean archivos temporales de una forma insegura. Un usuario malicioso local podría aprovechar este problema para realizar un ataque mediante un ataque simbólico, permitiendo sobrescribir contenidos de ficheros arbitrarios accesibles por la víctima que ejecuta los scripts.

También se solventan varios bugs que afectaban al funcionamiento normal de Bash.

Productos Afectados:

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 4 - i386, ia64, x86_64

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

Notas:

Se puede encontrar más información en:

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

Referencias en la web:

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

CVEs:

CVE-2008-5374

Servicios (ftp, www, dns, etc.) - Actualización de seguridad en sendmail

Fecha: 2/16/2011

Descripción:

Se ha producido un error en la forma en la que sendmail procesa los caracteres NUL en el campo CommonName de los certificados X.509. Un atacante podría ser capaz de obtener un certificado especialmente manipulado y que esté firmado por una Entidad certificadora de confianza, pudiendo conseguir que sendmail lo acepte por error y permita al atacante realizar un ataque de Man in The Middle o realizar un bypass de la autenticación por certificado.

Productos Afectados:

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 4 - i386, ia64, x86_64

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

Notas:

Se puede encontrar más información en:

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

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2011-0262.html>

CVEs:

CVE-2009-4565

Sistemas Operativos - Actualización de seguridad en Red Hat Cluster Suite 4

Fecha: 2/16/2011

Descripción:

El paquete de actualización permite que los nodos que fallen o que no sean alcanzables sean reiniciados de forma automática y borrados del cluster.

Se generan ficheros temporales inseguros. Este fallo se ha encontrado en fence_egenera, fence_apc, y fence_apc_snmp. Un atacante local podría utilizar estos problemas para sobrescribir ficheros arbitrarios escribibles por la víctima que ejecuta estas utilidades mediante un ataque por enlace simbólico.

Productos Afectados:

Red Hat Cluster Suite 4AS - i386, ia64, ppc, x86_64

Red Hat Cluster Suite 4ES - i386, ia64, x86_64

Red Hat Cluster Suite 4WS - i386, ia64, x86_64

Notas:

Se puede encontrar más información en:

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

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2011-0266.html>

CVEs:

CVE-2008-4192 CVE-2008-4579

Sistemas Operativos - Ampliación del soporte de Red Hat Enterprise Linux 4.7

Fecha: 2/16/2011

Descripción:

En acuerdo con la política erratas de soporte de RHEL, el soporte de actualizaciones extendido de RHEL4 update 7 terminará el 31 de Agosto.

Productos Afectados:

Red Hat Enterprise Linux AS version 4.7.z - i386, ia64, ppc, s390, s390x, x86_64

Red Hat Enterprise Linux ES version 4.7.z - i386, ia64, x86_64

Notas:

Se puede encontrar más información en:

<https://access.redhat.com/security/updates/classification/#low>

<https://access.redhat.com/support/policy/updates/errata/>

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2011-0279.html>

CVEs:

Aplicaciones Usuario - Actualización de Seguridad en java-1.6.0-openjdk

Fecha: 2/17/2011

Descripción:

Se ha detectado un problema en la librería swing. Los TimerEvents podrían utilizarse para saltarse las verificaciones el Security Manager, permitiendo el acceso a ficheros y directorios que, de otra forma, estarían inaccesibles.

Se ha detectado un problema en el componente HotSpot de Open JDK. Ciertas instrucciones bytecode confunden al administrador de memoria con la máquina virtual de Java, lo que podría producir una corrupción en el heap.

Se ha encontrado un problema en la forma en la que los componentes JAVXP son procesados, ya que podrían ser manipulados por applets que no son de confianza. Esto podría utilizarse para conseguir una elevación de privilegios y saltarse las restricciones de procesamiento de XML seguro.

Se ha detectado que el lanzador de Java proporcionado por OpenJDK no verifica la variable de entorno LD_LIBRARY_PATH para elementos inseguros y vacíos del path. Un atacante local podría ser capaz de convencer a un usuario para ejecutar el lanzador de Java mientras trabaja desde un directorio escribible por el atacante, pudiendo utilizarse este problema para cargar una librería que no es de confianza.

Se ha encontrado un problema en el componente de firma Digital XML en openJDK.

El código no verificado podría utilizar este problema para reemplazar firma digital XML del JRE, o las implementaciones del algoritmo C14N para interceptar las operaciones de firma digital.

Productos Afectados:

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

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

Red Hat Enterprise Linux Desktop (v. 6) - i386, x86_64

Red Hat Enterprise Linux Desktop Optional (v. 6) - i386, x86_64

Red Hat Enterprise Linux HPC Node (v. 6) - x86_64

Red Hat Enterprise Linux HPC Node Optional (v. 6) - x86_64

Red Hat Enterprise Linux Server (v. 6) - i386, x86_64

Red Hat Enterprise Linux Server Optional (v. 6) - i386, x86_64

Red Hat Enterprise Linux Workstation (v. 6) - i386, x86_64 Red Hat Enterprise Linux Workstation Optional (v. 6) - i386, x86_64

Notas:

Se puede encontrar más información en:

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

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2011-0281.html>

CVEs:

CVE-2010-4448 CVE-2010-4450 CVE-2010-4465 CVE-2010-4469 CVE-2010-4470 CVE-2010-4472

Aplicaciones Usuario - Actualización de seguridad en Java- 1-6-0

Fecha: 2/17/2011

Descripción:

La actualización soluciona varias vulnerabilidades en en Sun Java Runtime Environment y en el Sun Java 6 Software Development.

Productos Afectados:

Red Hat Desktop version 4 Extras - i386, x86_64

Red Hat Enterprise Linux AS version 4 Extras - i386, x86_64

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

Red Hat Enterprise Linux Desktop Supplementary (v. 6) - i386, x86_64

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

Red Hat Enterprise Linux HPC Node Supplementary (v. 6) - x86_64

Red Hat Enterprise Linux Server Supplementary (v. 5) - i386, x86_64

Red Hat Enterprise Linux Server Supplementary (v. 6) - i386, x86_64

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

Red Hat Enterprise Linux Workstation Supplementary (v. 6) - i386, x86_64

Notas:

Se puede encontrar más información en:

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

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2011-0282.html>

CVEs:

CVE-2010-4422 CVE-2010-4447 CVE-2010-4448 CVE-2010-4450 CVE-2010-4451 CVE-2010-4452 CVE-2010-4454 CVE-2010-4462 CVE-2010-4463 CVE-2010-4465 CVE-2010-4466 CVE-2010-4467 CVE-2010-4468 CVE-2010-4469 CVE-2010-4470 CVE-2010-4471 CVE-2010-4472 CVE-2010-4473 CVE-2010-4475 CVE-2010-4476

Sistemas Operativos - Validación de entrada insuficiente en telepathy gabble

Fecha: 2/16/2011

Descripción:

Se ha descubierto que telepathy Gabble, el administrador de conexiones de Jabber/XMPP del framework telepathy, está procesando actualizaciones google:jingleinfo sin validar su origen. Esto podría permitir a un atacante convertir el telepathy-gabble en un medio de datos streaming a través del servidor de su elección, e interceptar llamadas de vídeo o de audio.

Productos Afectados:

Versiones anteriores a la 0.7.6-1 en lenny

Versiones anteriores a la 0.9.15-1 en squeeze

Todas las versiones en wheezy

Notas:

Se puede encontrar más información en:

<http://www.debian.org/security/2011/dsa-2169>

Referencias en la web:

<http://www.debian.org/security/2011/dsa-2169>

CVEs:

Aplicaciones Usuario - Actualizaciones de seguridad en mailman

Fecha: 2/18/2011

Descripción:

Se han encontrado dos vulnerabilidades de Cross Site Scripting en Mailman. Un administrador de correo basado en web. Esto podría permitir a un atacante obtener las cookies de sesión insertando código javascript malicioso en los mensajes de confirmación, y en la lista del interfaz de admin.

Productos Afectados:

Versiones anteriores a la 1:2.1.11-11 en lenny

Versiones anteriores a la 1:2.1.13-5 en squeeze

Versiones anteriores a la 1:2.1.14-1 en wheezy

Notas:

Se puede encontrar más información en:

<http://www.debian.org/security/2011/dsa-2170>

Referencias en la web:

<http://www.debian.org/security/2011/dsa-2170>

CVEs:

CVE-2010-3089, CVE-2011-0707

Aplicaciones Usuario - Vulnerabilidad de seguridad en Asterisk

Fecha: 2/21/2011

Descripción:

Se ha descubierto una vulnerabilidad de buffer overflow en el canal SIP de Asterisk.
Se recomienda actualizar los paquetes de Asterisk.

Productos Afectados:

Versiones anteriores a la 1.4.21.2 en lenny
Versiones anteriores a la 1.6.2.9-2 en squeeze
Todas las versiones en sid

Notas:

Se puede encontrar más información en la URL de referencia.

Referencias en la web:

<http://www.debian.org/security/2011/dsa-2171>

CVEs:

CVE-2011-0495

Aplicaciones Usuario - Actualización de seguridad en java-1.4.2-ibm

Fecha: 2/22/2011

Descripción:

Se ha encontrado un problema de Denegación de Servicio en la forma en la que determinados strings se convierten en objetos double. Un atacante remoto podría utilizar este problema para causar un bloqueo de las aplicaciones Java.

Productos Afectados:

Red Hat Desktop version 4 Extras - i386, x86_64

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

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

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

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

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

Notas:

Se puede encontrar más información en:

<https://access.redhat.com/kb/docs/DOC-11259>

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2011-0292.html>

CVEs:

CVE-2010-4476

Aplicaciones Usuario - Actualización de Seguridad en Acroread

Fecha: 2/23/2011

Descripción:

Se han detectado varias vulnerabilidades en Adobe reader. Un fichero pdf especialmente modificado podría causar ataques de Cross Site Scripting (XSS) a través del usuario que abre el documento.

El fichero también podría causar el bloqueo de la aplicación así como permitir la ejecución de código arbitrario.

Productos Afectados:

Red Hat Desktop version 4 Extras - i386, x86_64

Red Hat Enterprise Linux AS version 4 Extras - i386, x86_64

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

Red Hat Enterprise Linux Desktop Supplementary (v. 6) - i386, x86_64

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

Red Hat Enterprise Linux Server Supplementary (v. 5) - i386, x86_64

Red Hat Enterprise Linux Server Supplementary (v. 6) - i386, x86_64

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

Red Hat Enterprise Linux Workstation Supplementary (v. 6) - i386, x86_64

Notas:

Se puede encontrar más información sobre la vulnerabilidad en:

<https://access.redhat.com/kb/docs/DOC-11259>

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2011-0301.html>

CVEs:

CVE-2011-0562 CVE-2011-0563 CVE-2011-0565 CVE-2011-0566 CVE-2011-0567 CVE-2011-0585 CVE-2011-0586 CVE-2011-0587 CVE-2011-0589 CVE-2011-0590 CVE-2011-0591 CVE-2011-0592 CVE-2011-0593 CVE-2011-0594 CVE-2011-0595 CVE-2011-0596 CVE-2011-0598 CVE-2011-0599 CVE-2011-0600 CVE-2011-0602 CVE-2011-0603 CVE-2011-0604 CVE-2011-0606

