

BOLETÍN DE VULNERABILIDADES
ÁUDEA, SEGURIDAD DE LA INFORMACIÓN
30 DE JUNIO 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 - RHTSA-2010:0474-01 - 6/15/2010 - Vulnerabilidades de seguridad en el Kernel**
- **Sistemas Operativos - HT4188/Apple - 6/15/2010 - Acerca del contenido de seguridad de la actualización de seguridad 2010-004 / Mac OS X v10.6.4**
- **Sistemas Operativos - RHTSA-2010:0488-01 - 6/16/2010 - Vulnerabilidad en Samba**
- **Aplicaciones Usuario - RHTSA-2010:0489-01 - 6/17/2010 - Vulnerabilidad de seguridad en java 1.5.0**
- **Sistemas Operativos - RHTSA-2010:0490-01 - 6/17/2010 - Vulnerabilidades en el sistema CUPS de los sistemas Red Hat**
- **Servicios (ftp, www, dns, etc.) - RHTSA-2010:0499-01 - 6/22/2010 - Actualización de seguridad en el navegador seamonkey**
- **Servicios (ftp, www, dns, etc.) - SUNBUG: 6898546**
- **SUNBUG: 6898539 - 6/22/2010 - Vulnerabilidad de seguridad en TLS (Transport Layer Security) y SSL3.0**
- **Sistemas Operativos - SUNBUG: 6857395 - 6/16/2010 - Vulnerabilidad de seguridad en la pila de Red de IPv6 sobre Solaris.**
- **Aplicaciones Usuario - SUNBUG: 6853745 - 6/17/2010 - Vulnerabilidad en el Sistema Sun Storage 7x00 2009 Q3**
- **Sistemas Operativos - SUNBUG: 6880764 - 6/26/2010 - Un problema en el reinicio podría generar problemas de integridad en el sistema de ficheros ZFS.**
- **Sistemas Operativos - SUNBUG 6518645 - 6/22/2010 - Bloqueos y reinicios en sistemas Solaris**
- **Sistemas Operativos - SUNBUG 6912703 - 6/19/2010 - Problemas en Solaris 10 tras la instalación de los parches 141444-09/141445-09**
- **Sistemas Operativos - Novell updates - 6/25/2010 - Publicación de actualizaciones de Novell**
- **Sistemas Operativos - VMSA-2010-0010 - 6/24/2010 - ESX 3.5 third party update for Service Console kernel**
- **Aplicaciones Usuario - MFSA 2010-26 Crítico - 6/22/2010 - Bloqueos con evidencia de corrupción de memoria (rv:1.9.2.4/ 1.9.1.10)**
- **Aplicaciones Usuario - MFSA 2010-27 Crítico - 6/22/2010 - Error use-after-free en nsCycleCollector::MarkRoots()**
- **Aplicaciones Usuario - MFSA 2010-28 Crítico - 6/22/2010 - Reutilización de objeto liberado a través de instancias del plugin**
- **Bases de Datos - MySQL Bug #53804 - 6/18/2010 - Problemas serios en el comando alter database**

- **Aplicaciones Usuario - MFSA 2010-30 Critico - 6/22/2010 - Overflow de entero in XSLT Node Sorting**
- **Aplicaciones Usuario - MFSA 2010-31 Moderado - 6/22/2010 - focus() puede ser utilizado para introducir o robar pulsaciones de teclado**
- **Aplicaciones Usuario - MFSA 2010-32 Moderado - 6/22/2010 - Content-Disposition: adjunto ignorado si Content-Type: multipart está también presente**
- **Aplicaciones Usuario - MFSA 2010-33 Bajo - 6/22/2010 - User tracking across sites using Math.random()**
- **Aplicaciones Usuario - APSB10-15 - 6/24/2010 - Actualizaciones de seguridad disponibles para Adobe Reader y Acrobat**

2. Boletín Detallado Vulnerabilidades

Sistemas Operativos - Vulnerabilidades de seguridad en el Kernel

Fecha: 6/15/2010

Descripción:

Se han publicado paquetes de actualización para solucionar 3 problemas de seguridad y varios errores en Red Hat Enterprise Linux 4. Las vulnerabilidades solucionadas son las siguientes:

-Se ha encontrado una referencia de un puntero NULL en la implementación Linux NFSv4. Varias de las funciones de bloqueo de ficheros de NFSv4 fallan al verificar si un fichero ha sido abierto en el servidor antes de realizar operaciones de bloqueo sobre él. Un usuario sin privilegios con una unidad compartida NFSv4 podría utilizar esta vulnerabilidad para causar una Denegación de Servicio (Kernel panic) o realizar una escalada de privilegios.

También se encontraron problemas en la función `sctp_process_unk_param()` del protocolo de transmisión de Stream del kernel de linux (SCTP). Un atacante remoto podría enviar un paquete SCTP especialmente diseñado a un puerto SCTP que esté escuchando del sistema objetivo, causando una Denegación de Servicio (kernel Panic).

Se ha encontrado un problema en una condición de "carrera" la búsqueda de un "keyring" por nombre y la destrucción de un "freed keyring". Este problema afecta al módulo de Administración de claves del kernel de linux. Un usuario local sin privilegios podría utilizar este problema para provocar una situación de de kernel panic (denegación de servicio) o realizar una escalada de privilegios.

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:

Los parches y actualizaciones e encuentran disponibles en la red Red Hat. Se puede encontrar más información sobre los mismos en:

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

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0474.html>

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

CVEs:

CVE-2009-3726 CVE-2010-1173 CVE-2010-1437

Sistemas Operativos - Acerca del contenido de seguridad de la actualización de seguridad 2010-004 / Mac OS X v10.6.4

Fecha: 6/15/2010

Descripción:

Se ha publicado una serie de actualizaciones para MAC OS X (versión 10.6.4).

Las actualizaciones involucran a los siguientes módulos:

- CUPS
- Desktop Services
- Plug-in de Flash Player
- Administrador de carpetas
- Visor de ayuda
- iChat
- ImageIO
- Kerberos
- libcurl
- Autorización de Red
- Open Directory
- Configuración de impresora
- Impresión
- Ruby
- Servidor de archivos SMB
- SquirrelMail
- Servidor wiki

Productos Afectados:

Windows 7, Vista, XP SP2 or later

Notas:

Se puede encontrar información más amplia y detallada sobre las vulnerabilidades descritas en el siguiente enlace:

http://support.apple.com/kb/HT4188?viewlocale=es_ES

Referencias en la web:

http://support.apple.com/kb/HT4188?viewlocale=es_ES

CVEs:

CVE-2010-0540 CVE-2010-0302 CVE-2010-1748 CVE-2010-0545 CVE-2010-0186 CVE-2010-0187 CVE-2010-0546 CVE-2010-1373 CVE-2010-1374 CVE-2010-0543 CVE-2009-4212 CVE-

2010-1320 CVE-2010-0283 CVE-2010-0734 CVE-2010-1375 CVE-2010-1376 CVE-2010-1377
CVE-2010-1379 CVE-2010-1380 CVE-2010-0541 CVE-2010-1381 CVE-2009-1578 CVE-2009-
1579 CVE-2009-1580 CVE-2009-1581 CVE-2009-2964 CVE-2010-1382

Sistemas Operativos - Vulnerabilidad en Samba

Fecha: 6/16/2010

Descripción:

Se ha encontrado una vulnerabilidad en la forma en la que Samba trata los datos parseados por el cliente. Un cliente malicioso podría enviar un paquete SMB especialmente diseñado al servidor Samba, resultando en una ejecución de código arbitrario. Con los privilegios del servidor Samba.

Productos Afectados:

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 (v. 5.3.z server) - i386, ia64, ppc, s390x, x86_64

Red Hat Enterprise Linux (v. 5.4.z 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 AS version 4.7.z - 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 ES version 4.7.z - 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 el parche publicado para solucionar el problema en:

<https://rhn.redhat.com/errata/RHSA-2010-0488.html>

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

Referencias en la web:

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

CVEs:

CVE-2010-2063

Aplicaciones Usuario - Vulnerabilidad de seguridad en java 1.5.0

Fecha: 6/17/2010

Descripción:

Se han encontrado varias vulnerabilidades en el entorno de desarrollo IBM Java 2 . Todas estas vulnerabilidades se pueden consultar en los siguientes enlaces:

<https://www.redhat.com/security/data/cve/CVE-2010-0840.html>

<https://www.redhat.com/security/data/cve/CVE-2010-0841.html>

<https://www.redhat.com/security/data/cve/CVE-2010-0842.html>

<https://www.redhat.com/security/data/cve/CVE-2010-0843.html>

<https://www.redhat.com/security/data/cve/CVE-2010-0844.html>

<https://www.redhat.com/security/data/cve/CVE-2010-0846.html>

<https://www.redhat.com/security/data/cve/CVE-2010-0847.html>

<https://www.redhat.com/security/data/cve/CVE-2010-0848.html>

<https://www.redhat.com/security/data/cve/CVE-2010-0849.html>

<http://www.redhat.com/security/updates/classification/#critical>

<http://www.ibm.com/developerworks/java/jdk/alerts/>

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:

Antes de aplicar las actualizaciones, se recomienda echar un vistazo a la información disponible en el siguiente enlace:

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

Referencias en la web:

<https://www.redhat.com/security/data/cve/CVE-2010-0840.html>

<https://www.redhat.com/security/data/cve/CVE-2010-0841.html>

<https://www.redhat.com/security/data/cve/CVE-2010-0842.html>

<https://www.redhat.com/security/data/cve/CVE-2010-0843.html>

<https://www.redhat.com/security/data/cve/CVE-2010-0844.html>

<https://www.redhat.com/security/data/cve/CVE-2010-0846.html>

<https://www.redhat.com/security/data/cve/CVE-2010-0847.html>

<https://www.redhat.com/security/data/cve/CVE-2010-0848.html>

<https://www.redhat.com/security/data/cve/CVE-2010-0849.html>

<http://www.redhat.com/security/updates/classification/#critical>

<http://www.ibm.com/developerworks/java/jdk/alerts/>

CVEs:

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 - Vulnerabilidades en el sistema CUPS de los sistemas Red Hat

Fecha: 6/17/2010

Descripción:

Se han publicado paquetes actualizados de CUPS que solventan las vulnerabilidades encontradas. Las vulnerabilidades son las siguientes:

-Se ha encontrado un fallo en la verificación de fallo de ubicación en memoria, provocando que un puntero apunte a NULL en el filtro "texttops". Un atacante podría crear un fichero de texto malicioso que cause la parada del servicio "texttops" o la ejecución de código arbitrario con los permisos del usuario "lp".

-Se ha encontrado una vulnerabilidad de Cross-Site Request Forgery (CSRF) en el interfaz web de CUPS. Si un atacante remoto consiguiera que un usuario validado como administrador visitase una página web especialmente diseñada, el atacante podría reconfigurar o deshabilitar CUPS, y conseguir acceso a los trabajos de impresión y a los ficheros del sistema.

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:

Los paquetes de actualización se encuentran disponibles en la red de Red Hat.

Se pueden encontrar más información sobre la red Red Hat, o sobre las actualizaciones en:

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

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0490.html>

CVEs:

CVE-2010-0540 CVE-2010-0542 CVE-2010-1748

Servicios (ftp, www, dns, etc.) - Actualización de seguridad en el navegador seamonkey

Fecha: 6/22/2010

Descripción:

Se han encontrado varias vulnerabilidades de seguridad en el navegador Seamonkey, relacionadas con la forma en la que seamonkey procesa el contenido web. Una página web que contenga contenido malicioso podría provocar que Seamonkey se bloquee, o se ejecute código arbitrario con los privilegios del usuario que ejecuta Seamonkey.

También se ha encontrado un problema en la forma en la que los plugins del navegador interactúan. Es posible que un plugin referencie el espacio de memoria de otro plugin, provocando la ejecución de código arbitrario con los permisos del usuario que ejecuta Seamonkey.

Por otro lado, también se ha descubierto un desbordamiento de cálculo entero al procesar una web con contenido malformado. Eso podría provocar que seamonkey se bloquee, o podría permitir la ejecución de código arbitrario.

También se ha descubierto una vulnerabilidad en los attachments de correo electrónico. Un mensaje de mail especialmente diseñado podría causar que Seamonkey se bloquee.

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:

Antes de aplicar los paquetes de actualización se recomienda ver la información publicada en el siguiente enlace sobre las actualizaciones:

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

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0499.html>

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

CVEs:

CVE-2010-0163 CVE-2010-1197 CVE-2010-1198 CVE-2010-1199 CVE-2010-1200

Servicios (ftp, www, dns, etc.) - Vulnerabilidad de seguridad en TLS (Transport Layer Security) y SSL3.0

Fecha: 6/22/2010

Descripción:

Se ha encontrado una vulnerabilidad de seguridad en TLS y SSL3.0 en la renegociación de sesiones, afectando a OpenSSL. Este problema podría permitir a un usuario remoto no autenticado, con la habilidad de interceptar y controlar el tráfico de red, realizar un ataque de Man in The Middle (MITM) e inyectar código arbitrario en texto plano al comienzo del stream del protocolo de aplicación, comprometiendo la integridad de la comunicación.

Productos Afectados:

SPARC Platform

Solaris 10 without patches 143140-04 and 145102-01

OpenSolaris based upon builds snv_01 through snv_128

x86 Platform

Solaris 10 without patch 141525-10

OpenSolaris based upon builds snv_01 through snv_128

Notas:

Solución: Instalar los siguientes paquetes de actualización:

SPARC Platform

Solaris 10 with patches 143140-04 or later and 145102-01 or later

OpenSolaris based upon builds snv_129 or later

x86 Platform

Solaris 10 with patch 141525-10 or later

OpenSolaris based upon builds snv_129 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-77-1021653.1-1>

CVEs:

CVE-2009-3555

Sistemas Operativos - Vulnerabilidad de seguridad en la pila de Red de IPv6 sobre Solaris.

Fecha: 6/16/2010

Descripción:

Se ha encontrado una vulnerabilidad de seguridad en la pila de red de IPv6 de Solaris que afecta al driver del dispositivo Cassini Gigabit-Ethernet, pudiendo causar una situación de "system panic" ante el ataque de un usuario remoto. Este ataque se categoriza como un tipo de Denegación de Servicio.

Productos Afectados:

SPARC platform

Solaris 10 without patch 141414-10

OpenSolaris based upon builds snv_01 through snv_82, and snv_111 through snv_123

x86 platform

Solaris 10 without patch 141415-10

OpenSolaris based upon builds snv_01 through snv_82, and snv_111 through snv_123

Notas:

Para solucionar el problema es importante instalar los siguientes paquetes de actualización:

SPARC Platform

Solaris 10 with patch 141414-10 or later

OpenSolaris based upon build snv_124 or later

x86 platform

Solaris 10 with patch 141415-10 or later

OpenSolaris based upon build snv_124 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-77-1020829.1-1>

CVEs:

Aplicaciones Usuario - Vulnerabilidad en el Sistema Sun Storage 7x00 2009 Q3

Fecha: 6/17/2010

Descripción:

En la versión 2009.Q3 del software existe un error que provoca un diagnóstico incorrecto de la CPU. Este diagnóstico indica la necesidad de realizar un reemplazo de hardware

Productos Afectados:

Sun Storage 7000 Unified Storage System

Sun Storage 7110 Unified Storage System

Sun Storage 7210 Unified Storage System

Sun Storage 7310 Unified Storage System

Sun Storage 7410 Unified Storage System

Notas:

Es importante instalar los siguientes paquetes de actualización:

Sun Storage 7x00 2009.Q3.4.1

Sun Storage 7x00 2010.Q1.0.0 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-77-1022237.1-1>

CVEs:

Sistemas Operativos - Un problema en el reinicio podría generar problemas de integridad en el sistema de ficheros ZFS.

Fecha: 6/26/2010

Descripción:

Al reiniciar la máquina, el renicio podría realizarse de forma abrupta, pudiendo afectar a la integridad en el sistema de ficheros ZFS, llagando a causar pérdidas de información.

Productos Afectados:

SPARC Platform

Solaris 10 with patch 142900-09 or later

OpenSolaris based upon builds snv_127 or later

x86 Platform

Solaris 10 with patch 142901-09 or later

OpenSolaris based upon builds snv_127 or later

Notas:

Para slventar el problema, se recomienda instalar los siguientes paquetes de actualizaciones:

SPARC Platform

Solaris 10 with patch 142900-09 or later

OpenSolaris based upon builds snv_127 or later

x86 Platform

Solaris 10 with patch 142901-09 or later

OpenSolaris based upon builds snv_127 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-77-1134162.1-1>

CVEs:

Sistemas Operativos - Bloqueos y reinicios en sistemas Solaris

Fecha: 6/22/2010

Descripción:

Se ha descubierto un problema en los sistemas Solaris con SVM configurado con "Root Mirrored", que podría provocar bloqueos y reinicios tras agregar un nuevo dispositivo.

Productos Afectados:

SPARC Platform

Solaris 10 with patch 127127-11 and without patch 143137-02

OpenSolaris based upon builds snv-65 though snv_124

x86 Platform

Solaris 10 with patch 127128-11 and without patch 143138-02

OpenSolaris based upon builds snv_65 though snv_124

Notas:

Solución: Instalar las siguientes actualizaciones:

SPARC Platform

Solaris 10 with patch 143137-02 or later

OpenSolaris based upon builds snv_125 or later

x86 Platform

Solaris 10 with patch 143138-02 or later

OpenSolaris based upon builds snv_125 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-77-1116047.1-1>

CVEs:

Sistemas Operativos - Problemas en Solaris 10 tras la instalación de los parches 141444-09/141445-09

Fecha: 6/19/2010

Descripción:

La instalación de los parches 141444-09/141445-09 en sistemas Solaris 10 podría causar que los LUNs EFI etiquetados no sean accesibles, devolviendo un error en los nodos presentes.

Productos Afectados:

SPARC Platform

Solaris 10 with patch 141444-09
x86 Platform

Solaris 10 with patch 141445-09

Notas:

Solución:

De momento la única solución existente consiste en desinstalar los parches 141444-09/141445-09

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-77-1124204.1-1>

CVEs:

Sistemas Operativos - Publicación de actualizaciones de Novell

Fecha: 6/25/2010

Descripción:

Se han publicado varias actualizaciones para diferentes módulos y programas de productos Novell.

- Actualización de perl-bootloader
- Actualización de seguridad para xmlrpc-c
- Actualización recomendada para yast2-webclient-systemtime
- Actualización de seguridad para SLMS
- Actualizaciones en servidores OES.

Productos Afectados:

-Perl bootloader:

- SUSE Linux Enterprise Desktop 11 SP1 for x86-64
- SUSE Linux Enterprise Desktop 11 SP1 for x86
- SUSE Linux Enterprise Server 11 SP1 for x86-64
- SUSE Linux Enterprise Server 11 SP1 for x86
- SUSE Linux Enterprise Server 11 SP1 for s390x
- SUSE Linux Enterprise Server 11 SP1 for ppc
- SUSE Linux Enterprise Server 11 SP1 for ia64

-xmlrpc-c:

- Linux Point of Service 9 for x86
- Open Enterprise Server (Linux) for x86
- 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

-yast2-webclient-systemtime

- WebYaST [Appliance - Tools] for x86-64
- WebYaST [Appliance - Tools] for x86

-SLMS:

- SUSE Lifecycle Management Server 1.0 [Appliance - Tools] for x86-64

Notas:

Todos los paquetes de actualización pueden descargarse desde la Web de descargas de Novell:

<http://download.novell.com/index.jsp>

Referencias en la web:

<http://download.novell.com/index.jsp>

CVEs:

Sistemas Operativos - ESX 3.5 third party update for Service Console kernel

Fecha: 6/24/2010

Descripción:

ESX 3.5 Console OS (COS) updates for COS package 'kernel'.

Productos Afectados:

VMware ESX 3.5 without patch ESX350-201006401-SG

Notas:

Referencias en la web:

<http://www.vmware.com/security/advisories/VMSA-2010-0010.html>

CVEs:

CVE-2008-5029 CVE-2008-5300 CVE-2009-1337 CVE-2009-1385 CVE-2009-1895 CVE-2009-2848 CVE-2009-3002 CVE-2009-3547 CVE-2009-2698 CVE-2009-2692

Aplicaciones Usuario - Bloqueos con evidencia de corrupción de memoria (rv:1.9.2.4/1.9.1.10)

Fecha: 6/22/2010

Descripción:

Los desarrolladores de Mozilla han identificado y solucionado varios fallos de estabilidad en el motor de navegación utilizado en Firefox y otros productos basados en Mozilla. Algunos de estos bloqueos mostraron evidencias de corrupción de memoria bajo ciertas circunstancias y se presume que con esfuerzo suficiente por lo menos algunos de los bloqueos podrían ser explotados para ejecutar código arbitrario.

Productos Afectados:

Firefox, Thunderbird, SeaMonkey

Notas:

Solucionado en Firefox 3.6.4, Firefox 3.5.10, Thunderbird 3.0.5, SeaMonkey 2.0.5

Referencias en la web:

<http://www.mozilla.org/security/announce/2010/mfsa2010-26.html>

<http://cve.mitre.org>

CVEs:

CVE-2010-1200, CVE-2010-1201, CVE-2010-1202, CVE-2010-1203

Aplicaciones Usuario - Error use-after-free en nsCycleCollector::MarkRoots()

Fecha: 6/22/2010

Descripción:

El investigador de seguridad wushi, de team509, ha reportado que el proceso de construcción de frames para ciertos tipos de menús podría dar como resultado un menú con un puntero apuntando a un objeto de menú liberado con anterioridad. Durante el proceso de recolección de ciclo, este elemento liberado podría ser accedido, resultando en la ejecución de una sección de código potencialmente controlada por el atacante.

Productos Afectados:

Firefox, SeaMonkey

Notas:

Solucionado en Firefox 3.5.10 y SeaMonkey 2.0.5

Referencias en la web:

<http://www.mozilla.org/security/announce/2010/mfsa2010-27.html>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0183>

CVEs:

CVE-2010-0183

Aplicaciones Usuario - Reutilización de objeto liberado a través de instancias del plugin

Fecha: 6/22/2010

Descripción:

Microsoft Vulnerability Research ha reportado que las instancias de dos plugins podrían interactuar de modo que un plugin obtiene una referencia a un objeto controlado por otro plugin y continua conservando esa referencia cuando el segundo plugin es desinstalado y el objeto eliminado. En esto casos, el primer plugin contendría un puntero a memoria liberada, que si es accedido, podría ser usado por un atacante para ejecutar código arbitrario en el equipo de la víctima.

Productos Afectados:

Firefox, SeaMonkey

Notas:

Solucionado en Firefox 3.6.4, Firefox 3.5.10, SeaMonkey 2.0.5

Referencias en la web:

<http://www.mozilla.org/security/announce/2010/mfsa2010-28.html>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1198>

CVEs:

CVE-2010-1198

Bases de Datos - Problemas serios en el comando alter database

Fecha: 6/18/2010

Descripción:

Un usuario con privilegios para ejecutar el comando alter database puede mover un directorio de sitio

Productos Afectados:

5.1.46, 5.1.48-bzr, 5.6.99-m4

Notas:

Referencias en la web:

<http://bugs.mysql.com/bug.php?id=53804>

CVEs:

Aplicaciones Usuario - Overflow de entero in XSLT Node Sorting

Fecha: 6/22/2010

Descripción:

El investigador de seguridad Martin Barbella ha reportado a través de TippingPoint's Zero Day Initiative que la rutina de orden de nodos XSLT contiene una vulnerabilidad de overflow de entero. Cuando uno de los nodos a ser ordenados contenía un valor de texto muy largo, el entero usado para reservar un buffer de memoria para almacenar su valor haría overflow, dando como resultado un buffer demasiado pequeño. Un atacante podría utilizar esta vulnerabilidad para escribir datos más allá del buffer, causando el bloqueo del navegador y potencialmente la ejecución de código arbitrario en el equipo de la víctima.

Productos Afectados:

Firefox, Thunderbird, SeaMonkey

Notas:

Solucionado en Firefox 3.6.4, Firefox 3.5.10, Thunderbird 3.0.5, SeaMonkey 2.0.5

Referencias en la web:

<http://www.mozilla.org/security/announce/2010/mfsa2010-30.html>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1199>

CVEs:

CVE-2010-1199

Aplicaciones Usuario - focus() puede ser utilizado para introducir o robar pulsaciones de teclado

Fecha: 6/22/2010

Descripción:

El investigador de seguridad de Google, Michael Zalewski, ha reportado que focus() puede ser utilizado para cambiar la ubicación del cursor de un usuario mientras escribe, dirigiendo potencialmente las entradas de su teclado hacia otra ubicación. Una web fraudulenta podría usar este comportamiento para robar pulsaciones de teclado de una víctima cuando está introduciendo datos sensibles como por ejemplo una contraseña.

Productos Afectados:

Firefox, SeaMonkey

Notas:

Solucionado en Firefox 3.6.4, Firefox 3.5.10, SeaMonkey 2.0.

Referencias en la web:

<http://www.mozilla.org/security/announce/2010/mfsa2010-31.html>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1125>

CVEs:

CVE-2010-1125

Aplicaciones Usuario - Content-Disposition: adjunto ignorado si Content-Type: multipart está también presente

Fecha: 6/22/2010

Descripción:

El investigador de seguridad Ilja van Sprundel, de IOActive, ha reportado que la cabecera HTTP Content-Disposition: attachment era ignorada cuando Content-Type: multipart estaba también presente. Este problema podría llevar potencialmente a un problema de XSS en webs que permitan al usuario subir ficheros arbitrarios y especificar un Content-Type pero apoyado en Content-Disposition: attachment para evitar que el contenido sea mostrado inline.

Productos Afectados:

Firefox, SeaMonkey

Notas:

Solucionado en Firefox 3.6.4, Firefox 3.5.10, SeaMonkey 2.0.5

Referencias en la web:

<http://www.mozilla.org/security/announce/2010/mfsa2010-32.html>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1197>

CVEs:

CVE-2010-1197

Aplicaciones Usuario - User tracking across sites using Math.random()

Fecha: 6/22/2010

Descripción:

El investigador de seguridad Amit Klein ha reportado que es posible hacer ingeniería inversa sobre el valor usado para el método Math.random(). Como el generador de números pseudo-aleatorio sólo era utilizado una vez por sesión de navegador, este valor de la semilla podría ser utilizado como token único para identificar y seguir a usuarios a través de diferentes webs.

Productos Afectados:

Firefox, SeaMonkey

Notas:

Solucionado en Firefox 3.6.4, Firefox 3.5.10, SeaMonkey 2.0.5

Referencias en la web:

<http://www.mozilla.org/security/announce/2010/mfsa2010-33.html>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5913>

CVEs:

CVE-2008-5913

Aplicaciones Usuario - Actualizaciones de seguridad disponibles para Adobe Reader y Acrobat

Fecha: 6/24/2010

Descripción:

Se han identificado vulnerabilidades críticas en Adobe Reader 9.3.2 (y versiones anteriores) para Windows, Macintosh y UNIX, Adobe Acrobat 9.3.2 (y versiones anteriores) para Windows y Macintosh, y Adobe Reader 8.2.2 (y versiones anteriores) y Adobe Acrobat 8.2.2 (y versiones anteriores) para Windows y Macintosh. Estas vulnerabilidades, incluyendo CVE-2010-1297 recogida en el Security Advisory APSA10-01, podría causar el bloqueo de la aplicación y potencialmente permitir a un atacante tomar el control sobre el equipo de la víctima.

Productos Afectados:

Adobe Reader 9.3.2 y versiones anteriores para Windows, Macintosh, y UNIX

Adobe Acrobat 9.3.2 y versiones anteriores para Windows y Macintosh

Notas:

Adobe recomienda a los usuarios de Adobe Reader 9.3.2 y versiones anteriores para Windows, Macintosh y UNIX que actualicen a Adobe Reader 9.3.3. (para usuarios de Adobe Reader en Windows y Macintosh que no puedan actualizar a Adobe Reader 9.3.3, Adobe ha facilitado la actualización Adobe Reader 8.2.3). Adobe recomienda a los usuarios de Adobe Acrobat 9.3.2 y versiones anteriores para Windows y Macintosh actualizar a Adobe Acrobat 9.3.3. Adobe recomienda a los usuarios de Adobe Acrobat 8.2.2 y versiones anteriores para Windows y Macintosh actualizar a Adobe Acrobat 8.2.3.

Referencias en la web:

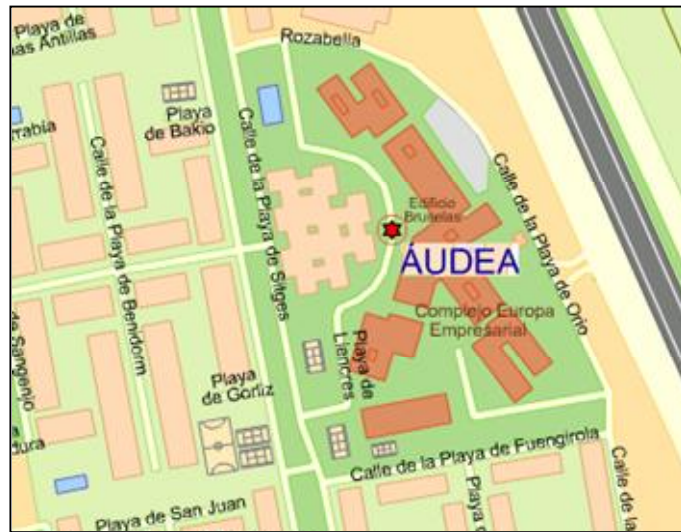
<http://www.adobe.com/support/security/bulletins/apsb10-15.html>

<http://cve.mitre.org>

CVEs:

CVE-2010-1240, CVE-2010-1285, CVE-2010-1295, CVE-2010-1297, CVE-2010-2168, CVE-2010-2201, CVE-2010-2202, CVE-2010-2203, CVE-2010-2204, CVE-2010-2205, CVE-2010-2206, CVE-2010-2207, CVE-2010-2208, CVE-2010-2209, CVE-2010-2210, CVE-2010-2211, CVE-2010-2212

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