

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

- Aplicaciones Usuario - 6910106 /Sun Microsystems - 2/18/2010 - **Vulnerabilidades den Solaris 10 IP Filter**
- Servicios (ftp, www, dns, etc.) - 6899619 /Sun Microsystems - 2/24/2010 - **Vulnerabilidades de seguridad en TLS y SSLv3**
- Aplicaciones Usuario - 6915746 /Sun Microsystems - 2/24/2010 - **Vulnerabilidad de Seguridad en Sun Java System Directory Server**
- Aplicaciones Usuario - 6877323 /Sun Microsystems - 2/25/2010 - **Varias Vulnerabilidades de desbordamiento de cálculo entero en Free Type 2**
- Servicios (ftp, www, dns, etc.) - 6840453 /Sun Microsystems - 2/25/2010 - **Vulnerabilidad de Seguridad en el módulo "modperl" de Apache 1.3**
- Sistemas Operativos - SUSE-SA:2010:013 - 2/19/2010 - **Actualizaciones en el Kernel de Novell Linux**
- Sistemas Operativos - SUSE-SR:2010:004 - 2/19/2010 - **Solventadas varias Vulnerabilidades en Suse**
- Sistemas Operativos - SUSE-SR:2010:004 - 2/23/2010 - **Solventadas varias Vulnerabilidades en Suse**
- Aplicaciones Usuario - MFSA 2010-01 Crítico - 2/17/2010 - **Bloqueos con evidencia de corrupción de memoria**
- Aplicaciones Usuario - MFSA 2010-02 Crítico - 2/17/2010 - **Vulnerabilidad de corrupción de memoria en Web Worker Array**
- Aplicaciones Usuario - MFSA 2010-03 Crítico - 2/17/2010 - **Bloqueo use-after-free en el parser HTML**
- Aplicaciones Usuario - MFSA 2010-04 Moderado - 2/17/2010 - **Riesgo de XSS en la llamada de tipo CrossDomain: Window.dialogArguments**
- Aplicaciones Usuario - MFSA 2010-05 Moderado - 2/17/2010 - **Riesgo de XSS usando documento SVG y Content-Type binario**
- Aplicaciones Usuario - APSB10-07 - 2/16/2010 - **Actualizaciones de seguridad disponibles para Adobe Reader y Acrobat**
- Aplicaciones Usuario - APSB10-08 - 2/23/2010 - **Actualización de seguridad para Adobe Download Manager**
- Aplicaciones Usuario - CA20100222-01 - 2/22/2010 - **Vulnerabilidad en Service Desk**
- Sistemas Operativos - VMSA-2010-0003 - 2/16/2010 - **Actualización de ESX Service Console para net-snmp**

## 2. Boletín Detallado Vulnerabilidades

### Aplicaciones Usuario - Vulnerabilidades den Solaris 10 IP Filter

Fecha: 2/18/2010

#### Descripción:

Algunos parches de Solaris 10 IP Filter podría provocar una fuga de memoria en los sistemas con el "Stateful Filtering" configurado.

#### Productos Afectados:

SPARC Platform

Solaris 8

Solaris 9

Solaris 10

OpenSolaris based upon builds snv\_01 through snv\_132

x86 Platform

Solaris 8

Solaris 9

Solaris 10

OpenSolaris based upon builds snv\_01 through snv\_132

#### Notas:

Solución:

SPARC Platform

Solaris 10 with patch 141506-05 or 141506-06 and without patch 141506-07

x86 Platform

Solaris 10 with patch 141505-05 or 141505-06 and without patch 141505-07

#### Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-275590-1>

#### CVEs:



## **Servicios (ftp, www, dns, etc.) - Vulnerabilidades de seguridad en TLS y SSLv3**

**Fecha:** 2/24/2010

### **Descripción:**

Una vulnerabilidad de seguridad en TLS y SSLv3 realiza renegociaciones tras el primer handshake, lo que podría permitir un ataque Man in The middle por parte de un atacante.

### **Productos Afectados:**

Sun Java System Web Server 6.1

Sun Java System Web Server 7.0

Sun Java System Web Proxy Server 4.0

Sun Java System Application Server Enterprise Edition 8.2

Sun GlassFish Enterprise Server v2.1

Sun Java System Directory Server 5.2

Sun Java System Directory Server Enterprise Edition 6.0

Sun Java System Directory Server Enterprise Edition 6.1

Sun Java System Directory Server Enterprise Edition 6.2

Sun Java System Directory Server Enterprise Edition 6.3

### **Notas:**

**Solución:**

#### **SPARC Platform**

Sun Java System Web Server 6.1 with patch 116648-24 or later

Sun Java System Web Server 6.1 with Service Pack 12 or later

Sun Java System Web Server 7.0 with patch 125437-18 or later

Sun Java System Web Server 7.0 update 7 or later

Sun Java System Web Proxy Server 4.0 through 4.0.12 with patch 120981-20 or later

Sun Java System Application Server 8.1 (Enterprise Edition SVR4) with patch 119166-40 or later

Sun Java System Application Server 8.1 (Enterprise Edition file based) with patch 119169-33 or later

Sun Java System Application Server 8.2 (Enterprise Edition File Based) with patch 124675-13 or later

Sun GlassFish Enterprise Server v2.1.1 with HADB - Package Based with patch 128640-15 or later (for customers with valid support contract) or 141709-03 or later for customers without valid support contract)

Sun GlassFish Enterprise Server v2.1.1 with HADB with patch 128643-15 or later (for customers with valid support contract) or 141700-03 or later (for customers without valid support contract)

#### **x86 Platform**

Sun Java System Web Server 6.1 with patch 116649-24 or later  
Sun Java System Web Server 6.1 with Service Pack 12 or later  
Sun Java System Web Server 7.0 with patch 125438-18 or later  
Sun Java System Web Server 7.0 update 7 or later  
Sun Java System Web Proxy Server 4.0 through 4.0.12 with patch 120982-20 or later  
Sun Java System Application Server 8.1 (Enterprise Edition SVR4) with patch 119167-40 or later  
Sun Java System Application Server 8.1 (Enterprise Edition file based) with patch 119170-33 or later  
Sun Java System Application Server 8.2 (Enterprise Edition File Based) with patch 124676-13 or later  
Sun GlassFish Enterprise Server v2.1.1 with HADB - Package Based with patch 128641-15 or later (for customers with valid support contract) or 141710-03 or later (for customers without valid support contract)  
Sun GlassFish Enterprise Server v2.1.1 with HADB with patch 128644-15 or later (for customers with valid support contract) or 141701-03 or later (for customers without valid support contract)

#### Linux

Sun Java System Web Server 6.1 with patch 118202-16 or later  
Sun Java System Web Server 6.1 with Service Pack 12 or later  
Sun Java System Web Server 7.0 with patch 125439-16 or later  
Sun Java System Web Server 7.0 update 7 or later  
Sun Java System Web Proxy Server 4.0 through 4.0.12 with patch 120983-20 or later  
  
Sun Java System Application Server 8.1 (Enterprise Edition Package Based) with patch 119168-40 or later  
  
Sun Java System Application Server 8.1 (Enterprise Edition File Based) with patch 119171-33 or later  
Sun Java System Application Server 8.2 (Enterprise Edition File Based) with patch 124677-13 or later  
Sun GlassFish Enterprise Server v2.1.1 with HADB - Package Based with patch 128642-15 or later (for customers with valid support contract) or 141711-03 or later (for customers without valid support contract)  
Sun GlassFish Enterprise Server v2.1.1 with HADB with patch 128645-15 or later (for customers with valid support contract) or 141702-03 or later (for customers without valid support contract)

#### HP-UX

Sun Java System Web Server 6.1 with patch 121510-08 or later  
Sun Java System Web Server 6.1 with Service Pack 12 or later  
Sun Java System Web Server 7.0 with patch 125440-16 or later  
Sun Java System Web Server 7.0 update 7 or later  
Sun Java System Web Proxy Server 4.0 through 4.0.12 with patch 123532-09 or later

## Windows

Sun Java System Web Server 6.1 with patch 121524-08 or later

Sun Java System Web Server 6.1 with Service Pack 12 or later

Sun Java System Web Server 7.0 with patch 125441-18 or later

Sun Java System Web Server 7.0 update 7 or later

Sun Java System Web Proxy Server 4.0 through 4.0.12 with patch 126325-10 or later

Sun Java System Application Server 8.1 (Enterprise Edition Package based) with patch 122848-25 or later

Sun Java System Application Server 8.1 (Enterprise Edition File Based) with patch 119172-33 or later

Sun Java System Application Server 8.2 (Enterprise Edition File Based) with patch 124678-13 or later

Sun GlassFish Enterprise Server v2.1.1 with HADB with patch 128646-15 or later (for customers with valid support contract) or 141703-03 or later (for customers without valid support contract)

## Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-274990-1>

## CVEs:

## **Aplicaciones Usuario - Vulnerabilidad de Seguridad en Sun Java System Directory Server**

**Fecha:** 2/24/2010

### **Descripción:**

Una vulnerabilidad en Java System Directory Server podría permitir consultas especialmente diseñadas contra el LDAP, causando una denegación de servicio.

### **Productos Afectados:**

Sun Directory Server Enterprise Edition  
Sun Java System Directory Server Enterprise Edition 6.3  
Sun Java System Directory Server Enterprise Edition 6.2  
Sun Java System Directory Server Enterprise Edition 6.1  
Sun Java System Directory Server Enterprise Edition 6.0  
Sun Java System Directory Server 5.2

### **Notas:**

**Solución:**

Instalar los siguientes parches:

Sun Directory Server Enterprise Edition 7.0 with patch 143884-01 or later

Sun Java System Directory Server Enterprise Edition 6.3.1 with patch 143463-01 or later

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

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-275711-1>

**CVEs:**

## **Aplicaciones Usuario - Varias Vulnerabilidades de desbordamiento de cálculo entero en Free Type 2**

**Fecha:** 2/25/2010

### **Descripción:**

Se han descubierto varias vulnerabilidades en la librería de fuentes FreeType2 (libfreetype) que podría afectar a las aplicaciones que hagan uso de ella. Dependiendo de la aplicación, la vulnerabilidad podría permitir a un usuario local, o remoto sin privilegios provocar un bloqueo de la aplicación utilizando un fichero de fuente especialmente diseñado, y provocando como resultado una denegación del Servicio.

### **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:**

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-270268-1>

**CVEs:**

## Servicios (ftp, www, dns, etc.) - Vulnerabilidad de Seguridad en el módulo "modperl" de Apache 1.3

Fecha: 2/25/2010

### Descripción:

El módulo "modperl" de Apache 1.3 es vulnerable a ataques de Cross Site Scripting, permitiendo que usuarios remotos sin privilegios inyectar código web arbitrario mientras se visita una URL especialmente diseñada para aprovechar la vulnerabilidad, pudiendo obtener las credenciales de usuario, o realizar un session hijacking.

### Productos Afectados:

SPARC Platform

Solaris 8

Solaris 9

Solaris 10 without patch 122911-18

OpenSolaris based upon builds snv\_01 through snv\_116

x86 Platform

Solaris 8

Solaris 9

Solaris 10 without patch 122912-18

OpenSolaris based upon builds snv\_01 through snv\_116

### Notas:

Instalar los siguientes parches:

SPARC Platform

Solaris 10 with patch 122911-18 or later

OpenSolaris based upon builds snv\_117 or later

x86 Platform

Solaris 10 with patch 122912-18 or later

OpenSolaris based upon builds snv\_117 or later

Está pendiente una publicación de parches para Solaris 8 y 9.

### Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-274110-1>

**CVEs:**

## Sistemas Operativos - Actualizaciones en el Kernel de Novell Linux

Fecha: 2/19/2010

### Descripción:

Se han solventado numerosos problemas presentes en la versión anterior. Dichos problemas se listan a continuación, ordenados por CVE:

CVE-2009-4005: The collect\_rx\_frame function in drivers/isdn/hisax/hfc\_usb.c in the Linux kernel allows attackers to have an unspecified impact via a crafted HDLC packet that arrives over ISDN and triggers a buffer under-read.

CVE-2009-3080: Array index error in the gdth\_read\_event function in drivers/scsi/gdth.c in the Linux kernel allows local users to cause a denial of service or possibly gain privileges via a negative event index in an IOCTL request.

CVE-2010-0007: Missing CAP\_NET\_ADMIN checks in the ebttables netfilter code might have allowed local attackers to modify bridge firewall settings.

CVE-2009-4536: drivers/net/e1000/e1000\_main.c in the e1000 driver in the Linux kernel handles Ethernet frames that exceed the MTU by processing certain trailing payload data as if it were a complete frame, which allows remote attackers to bypass packet filters via a large packet with a crafted payload.

CVE-2009-3889: The dbg\_lvl file for the megaraid\_sas driver in the Linux kernel has world-writable permissions, which allows local users to change the (1) behavior and (2) logging level of the driver by modifying this file.

CVE-2009-1883: The z90crypt\_unlocked\_ioctl function in the z90crypt driver in the Linux kernel does not perform a capability check for the Z90QUIESCE operation, which allows local users to leverage euid 0 privileges to force a driver outage.

CVE-2009-2903: Memory leak in the appletalk subsystem in the Linux kernel, when the appletalk and ipddp modules are loaded but the

ipddp"N" device is not found, allows remote attackers to cause a denial of service (memory consumption) via IP-DDP datagrams.

CVE-2009-3621: net/unix/af\_unix.c in the Linux kernel allows local users to cause a denial of service (system hang) by creating an abstract-namespace AF\_UNIX listening socket, performing a shutdown operation on this socket, and then performing a series of connect operations to this socket.

CVE-2009-3620: The ATI Rage 128 (aka r128) driver in the Linux kernel does not properly verify Concurrent Command Engine (CCE) state initialization, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly gain privileges via unspecified ioctl calls.

#### **Productos Afectados:**

SUSE Linux Enterprise 9

#### **Notas:**

Los enlaces para descargar las actualizaciones son los siguientes:

SUSE CORE 9 for Itanium Processor Family

[http://download.novell.com/index.jsp?search=Search&set\\_restricted=true&keywords=f244ff5c3b3396176b5103f1715e6684](http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=f244ff5c3b3396176b5103f1715e6684)

SUSE CORE 9 for IBM zSeries 64bit

[http://download.novell.com/index.jsp?search=Search&set\\_restricted=true&keywords=a31f023a60d07c8888e454fa1d125def](http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=a31f023a60d07c8888e454fa1d125def)

SUSE CORE 9 for IBM S/390 31bit

[http://download.novell.com/index.jsp?search=Search&set\\_restricted=true&keywords=687ae9e3794e96759e414f98fbdce2b2](http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=687ae9e3794e96759e414f98fbdce2b2)

SUSE CORE 9 for AMD64 and Intel EM64T

[http://download.novell.com/index.jsp?search=Search&set\\_restricted=true&keywords=4267d3a69718225e2fb2c25170bc6d94](http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=4267d3a69718225e2fb2c25170bc6d94)

#### Novell Linux POS 9

[http://download.novell.com/index.jsp?search=Search&set\\_restricted=true&keywords=115c23c0f70fab25bce4f2dedb036c6c](http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=115c23c0f70fab25bce4f2dedb036c6c)

#### SUSE CORE 9 for x86

[http://download.novell.com/index.jsp?search=Search&set\\_restricted=true&keywords=115c23c0f70fab25bce4f2dedb036c6c](http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=115c23c0f70fab25bce4f2dedb036c6c)

#### SUSE SLES 9

[http://download.novell.com/index.jsp?search=Search&set\\_restricted=true&keywords=f244ff5c3b3396176b5103f1715e6684](http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=f244ff5c3b3396176b5103f1715e6684)

[http://download.novell.com/index.jsp?search=Search&set\\_restricted=true&keywords=a31f023a60d07c8888e454fa1d125def](http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=a31f023a60d07c8888e454fa1d125def)

[http://download.novell.com/index.jsp?search=Search&set\\_restricted=true&keywords=687ae9e3794e96759e414f98fbdce2b2](http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=687ae9e3794e96759e414f98fbdce2b2)

[http://download.novell.com/index.jsp?search=Search&set\\_restricted=true&keywords=4267d3a69718225e2fb2c25170bc6d94](http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=4267d3a69718225e2fb2c25170bc6d94)

[http://download.novell.com/index.jsp?search=Search&set\\_restricted=true&keywords=115c23c0f70fab25bce4f2dedb036c6c](http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=115c23c0f70fab25bce4f2dedb036c6c)

[http://download.novell.com/index.jsp?search=Search&set\\_restricted=true&keywords=07c0f8cc874baafd99ac348e3dc688c7](http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=07c0f8cc874baafd99ac348e3dc688c7)

#### SUSE CORE 9 for IBM POWER

[http://download.novell.com/index.jsp?search=Search&set\\_restricted=true&keywords=07c0f8cc874baafd99ac348e3dc688c7](http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=07c0f8cc874baafd99ac348e3dc688c7)

#### Referencias en la web:

[http://www.novell.com/linux/security/advisories/2010\\_13\\_kernel.html](http://www.novell.com/linux/security/advisories/2010_13_kernel.html)

#### CVEs:

CVE-2009-1883, CVE-2009-2903, CVE-2009-3080, CVE-2009-3620, CVE-2009-3621, CVE-2009-3889, CVE-2009-4005, CVE-2009-4536, CVE-2010-0007

## Sistemas Operativos - Solventadas varias Vulnerabilidades en Suse

Fecha: 2/19/2010

### Descripción:

Se han solventado vulnerabilidades presentes en los siguientes módulos:

- moodle
- xpdf
- pdns-recursor
- pango
- horde
- gnome-screensaver
- fuse
- gnutls
- flash-player

A continuación se describen los puntos solventados:

#### - moodle

This patch updates Moodle to the latest stable upstream version (1.9.7)

fixing multiple security issues:

CVE-2009-4297, CVE-2009-4298, CVE-2009-4299, CVE-2009-4300,  
CVE-2009-4301, CVE-2009-4302, CVE-2009-4303, CVE-2009-4304,  
CVE-2009-4305, MSA-09-0030

(New detection of insecure Flash player plugins)

The new version also has a completely new , more secure password handling.

Beside other features, Admins will be asked to change their passwords next time they log in after upgrading.

Affected products: openSUSE 11.0-11.1

#### - xpdf

This update of xpdf fixes an integer overflow that may lead to code execution. (CVE-2009-4035: CVSS v2 Base Score: 6.8)

Affected products: SLES SDK 9

#### - pdns-recursor

This update of pdns-recursor improves the packet parsing code to fix a possible DNS spoofing vulnerability (CVE-2009-4010) and a remote buffer overflow that could give the ability to execute arbitrary code (CVE-2009-4009).

Affected products: openSUSE 11.0-11.2

- pango

Long glyph string could trigger a heap-based buffer overflow in pango (CVE-2009-1194).

Affected products: openSUSE 11.0-11.1, NLD9, SLES9, SLE10, SLE11

- horde

This update of horde fixes:

- CVE-2009-3236: CVSS v2 Base Score: 5.0: Overwrite arbitrary files and execute PHP code

- CVE-2009-3237: CVSS v2 Base Score: 5.0: Cross-Site Scripting (XSS)

- CVE-2009-3701: CVSS v2 Base Score: 4.3: Cross-Site Scripting (XSS)

- CVE-2009-4363: CVSS v2 Base Score: 4.3: Cross-Site Scripting (XSS)

Affected products: openSUSE 11.0

- gnome-screensaver

gnome-screensaver was updated to the stable release 2.28.3, fixing various bugs and security issues.

Following security issues have been fixed:

When resuming a system gnome-screensaver does not lock external displays that got connected while the system was suspended (CVE-2010-0285: CVSS v2 Base Score: 5.6).

Additionally another bug in gnome-screensaver was fixed that allowed bypassing the unlock dialog by using a removable monitor. (CVE-2010-0414: CVSS v2 Base Score: 6.2)

Pressing "return" repeatedly caused a X error which terminated the lock and so allowed local users to access the underlying session.

CVE-2010-0422: gnome-screensaver can lose its keyboard grab when locked, exposing the system to intrusion by adding and removing monitors.

Affected products: openSUSE 11.1-11.2

- fuse

A race condition in fusermount allowed users to umount any filesystem (CVE-2009-3297).

Affected products: SLE SDK 10, SLED10

- gnutls

gnutls did not properly handle embedded '\0' characters in x509 certificates. Attackers using specially crafted certificates could exploit that to conduct man-in-the-middle attacks (CVE-2009-2730).

Affected products: openSUSE 11.2

- flash-player

Insufficient checks in flash-player allowed malicious flash applets to create illegal cross-domain requests (CVE-2010-0186). The update also fixes a denial of service condition (CVE-2010-0187).

Affected products: 11.0-11.2, SLE10, SLE11

#### **Productos Afectados:**

openSUSE 11.0-11.1

SLES SDK 9

openSUSE 11.0-11.2

openSUSE 11.0-11.1

NLD9

SLES9

SLE10

SLE11

#### **Notas:**

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

[http://www.novell.com/linux/security/advisories/2010\\_4\\_sr.html](http://www.novell.com/linux/security/advisories/2010_4_sr.html)

#### **CVEs:**

CVE-2009-1194, CVE-2009-2730, CVE-2009-3236, CVE-2009-3237, CVE-2009-3297, CVE-2009-3701, CVE-2009-4009, CVE-2009-4010, CVE-2009-4035, CVE-2009-4297, CVE-2009-4298, CVE-2009-4299, CVE-2009-4300, CVE-2009-4301, CVE-2009-4302 CVE-2009-4303, CVE-2009-4304, CVE-2009-4305, CVE-2009-4363, CVE-2010-0186, CVE-2010-0187, CVE-2010-0285, CVE-2010-0414, CVE-2010-0422

## Sistemas Operativos - Solventadas varias Vulnerabilidades en Suse

Fecha: 2/23/2010

### Descripción:

Se han solventado vulnerabilidades presentes en los siguientes módulos:

- fetchmail
  - krb5
  - rubygem-actionpack-2\_1
  - libexpat0
  - unbound
  - apache2-mod\_php5/php5

### Productos Afectados:

openSUSE 11.1-11.2

### Notas:

### Referencias en la web:

[http://www.novell.com/linux/security/advisories/2010\\_5\\_sr.html](http://www.novell.com/linux/security/advisories/2010_5_sr.html)

### CVEs:

CVE-2008-5624, CVE-2008-5625, CVE-2008-5814, CVE-2008-7248, CVE-2009-2625, CVE-2009-2626, CVE-2009-2687, CVE-2009-3546, CVE-2009-3560, CVE-2009-3602, CVE-2009-4017, CVE-2009-4142, CVE-2009-4214, CVE-2010-0283, CVE-2010-0562

## **Aplicaciones Usuario - Bloqueos con evidencia de corrupción de memoria**

**Fecha:** 2/17/2010

### **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

SeaMonkey

### **Notas:**

Deshabilitar JavaScript hasta que se pueda instalar una versión que contenga estas soluciones.

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

<http://www.mozilla.org/security/announce/2010/mfsa2010-01.html>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0159>

### **CVEs:**

CVE-2010-0159

## **Aplicaciones Usuario - Vulnerabilidad de corrupción de memoria en Web Worker Array**

**Fecha:** 2/17/2010

### **Descripción:**

El investigador de Seguridad Orlando Barrera II ha reportado a través de la iniciativa Zero Day de TippingPoint que la implementación de Mozilla de los Web Wrokers contienen un error en la gestión de tipos de datos array al procesar mensajes posteados. Este error podría ser usado por un atacante para provocar una corrupción de memoria y bloquear el navegador, pudiendo ejecutar código arbitrario en el ordenador de la víctima.

Los Web Workers fueron introducidos en Firefox 3.5; Firefox 3.0 y versiones anteriores de Firefox no se ven afectadas.

### **Productos Afectados:**

Firefox  
SeaMonkey

### **Notas:**

Deshabilitar JavaScript hasta que se pueda instalar una versión que contenga estas soluciones.

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

<http://www.mozilla.org/security/announce/2010/mfsa2010-02.html>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0160>

### **CVEs:**

CVE-2010-0160

## **Aplicaciones Usuario - Bloqueo use-after-free en el parser HTML**

**Fecha:** 2/17/2010

### **Descripción:**

El investigador de seguridad Alin Rad Pop, de Secunia Research ha reportado que el parser HTML liberó incorrectamente memoria usada cuando había espacio insuficiente para procesar las entradas restantes. En esas circunstancias la memoria ocupada por objetos en uso era liberada y podía ser luego ocupada con texto controlado por el atacante. Estas condiciones podrían resultar en la ejecución de código arbitrario si los metodos en los objetos liberados fueran posteriormente invocados.

### **Productos Afectados:**

Firefox

SeaMonkey

### **Notas:**

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

<http://www.mozilla.org/security/announce/2010/mfsa2010-02.html>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1571>

### **CVEs:**

CVE-2009-1571

## **Aplicaciones Usuario - Riesgo de XSS en la llamada de tipo CrossDomain: Window.dialogArguments**

Fecha: 2/17/2010

### **Descripción:**

El investigador de seguridad Hidetake Jo de Microsoft Vulnerability Research ha reportado que las propiedades establecidas en un objeto pasado a showModalDialog pueden ser leídas por el documento contenido en el diálogo, incluso cuando el documento es leído desde un dominio diferente. Esto es una violación de la política de mismo origen y podría provocar que un website ejecutara JavaScript no confiable si asume que dialogArguments no pudo ser inicializado por otro sitio web.

### **Productos Afectados:**

Firefox

SeaMonkey

### **Notas:**

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

<http://www.mozilla.org/security/announce/2010/mfsa2010-04.html>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3988>

### **CVEs:**

CVE-2009-3988

## **Aplicaciones Usuario - Riesgo de XSS usando documento SVG y Content-Type binario**

**Fecha:** 2/17/2010

### **Descripción:**

El investigador de seguridad de Mozilla George Guninski ha reportado que cuando un documento SVG que es servido con Content-Type: application/octet-stream es incluido en otro documento a través del tag <embed> con type="image/svg+xml", el Content-Type es ignorado y el documento SVG es procesado normalmente. Un website que permita la subida de datos binarios arbitrarios pero que se basa en Content-Type: application/octet-stream para prevenir la ejecución de scripts podría ver superada esa protección.

### **Productos Afectados:**

Firefox

SeaMonkey

### **Notas:**

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

<http://www.mozilla.org/security/announce/2010/mfsa2010-05.html>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0162>

### **CVEs:**

CVE-2010-0162

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

**Fecha:** 2/16/2010

### **Descripción:**

Se ha identificado una vulnerabilidad grave en Adobe Reader 9.3 para Windows, Macintosh y Unix, en Adobe Acrobat 9.3 para Windows y Macintosh, y en Adobe Reader 8.2 y Acrobat 8.2 para Windows y Macintosh. Tal y como se describe en el Boletín de seguridad APSB10-06, dicha vulnerabilidad (CVE-2010-0186) podría trastornar el dominio de Sandbox y realizar solicitudes de varios dominios no autorizados. Además, se ha identificado una vulnerabilidad grave (CVE-2010-0188) que podría provocar que la aplicación se bloquee y podría permitir que un intruso se hiciera con el control del sistema afectado.

### **Productos Afectados:**

Adobe Reader 9.3 y versiones anteriores para Windows, Macintosh y UNIX

Adobe Acrobat 9.3 y versiones anteriores para Windows y Macintosh

### **Notas:**

Adobe recomienda a los usuarios de Adobe Reader 9.3 y las versiones anteriores para Windows, Macintosh y UNIX que actualicen a Adobe Reader 9.3.1. (Para los usuarios de Adobe Reader de Windows y Macintosh que no puedan actualizar a Adobe Reader 9.3.1, Adobe ha proporcionado la actualización de Adobe Reader 8.2.1). Adobe recomienda a los usuarios de Adobe Reader 9.3 y las versiones anteriores para Windows y Macintosh que actualicen a Adobe Reader 9.3.1. Adobe recomienda a los usuarios de Acrobat 8.2 y las versiones anteriores para Windows y Macintosh que actualicen a Acrobat 8.2.1.

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

<http://www.adobe.com/es/support/security/bulletins/apsb10-07.html>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0186>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188>

### **CVEs:**

CVE-2010-0188, CVE-2010-0186

## Aplicaciones Usuario - Actualización de seguridad para Adobe Download Manager

Fecha: 2/23/2010

### Descripción:

Una vulnerabilidad crítica ha sido identificada en Adobe Download Manager, versiones 1.6.2.60 y anteriores para Windows. Esta vulnerabilidad (CVE-2010-0189) podría potencialmente permitir a un atacante descargar e instalar software no autorizado en el equipo de un usuario.

### Productos Afectados:

Adobe Download Manager versiones 1.6.2.60 y anteriores para Windows (antes del 23 Febrero de 2010)

### Notas:

Los usuarios que hayan descargado Adobe Reader Windows desde <http://get.adobe.com/reader/> o Adobe Flash Player para Windows desde <http://get.adobe.com/flashplayer/> con anterioridad al lanzamiento de este Security Bulletin el 23 de Febrero de 2010, pueden verificar que no son vulnerables a este problema de Adobe Download Manager siguiendo las instrucciones en la sección Solución.

### Referencias en la web:

<http://www.adobe.com/support/security/bulletins/apsb10-08.html>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0189>

### CVEs:

CVE-2010-0189

## **Aplicaciones Usuario - Vulnerabilidad en Service Desk**

**Fecha:** 2/22/2010

### **Descripción:**

La versión de tomcat incluida en CA Service Desk R12.1 es vulnerable a un ataque cross-site scripting.

### **Productos Afectados:**

CA Service Desk r12.1 en plataforma Windows y Unix

### **Notas:**

Se pueden seguir las instrucciones del documento TEC503137 para determinar si una instalación es vulnerable y corregir el problema.

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

<https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=229526>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1947>

### **CVEs:**

CVE-2008-1947

## Sistemas Operativos - Actualización de ESX Service Console para net-snmp

Fecha: 2/16/2010

### Descripción:

Esta actualización soluciona un error de división por cero en el demonio snmpd. Un atacante remoto podría realizar una petición GETBULK que podría causar que el demonio fallara.

### Productos Afectados:

VMware ESX 3.5 without patch ESX350-201002401-SG

### Notas:

El parche/versión para cada producto se puede descargar de:

ESX 3.5 ----- ESX350-201002401-SG  
<http://download3.vmware.com/software/vi/ESX350-201002401-SG.zip>  
md5sum: a91428cb6bc2da794f581aefd5eef010  
<http://kb.vmware.com/kb/1017660>

### Referencias en la web:

<http://www.vmware.com/security/advisories/VMSA-2010-0003.html>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1887>

### CVEs:

CVE-2009-1887

**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](http://www.audea.com)  
[info@audea.com](mailto:info@audea.com)