

BOLETÍN DE VULNERABILIDADES
ÁUDEA, SEGURIDAD DE LA INFORMACIÓN
31 DE ENERO 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

- Aplicaciones Usuario - 6755033 /Sun Microsystems - 1/18/2010 - Fallo en la reconfiguración dinámica de Sun StorageTek VM/HSC
- Sistemas Operativos - 6759500 /Sun Microsystems - 1/19/2010 - Varias Vulnerabilidades en Solaris relacionadas con TCP podrían provocar condiciones de Denegación del Servicio
- Aplicaciones Usuario - - 1/20/2010 - Vulnerabilidad de Cross Site Scripting en el Servidor de Mensajes de Java
- Aplicaciones Usuario - 6639618 /Sun Microsystems - 1/20/2010 - Fallo en los comandos de reserva persistente
- Aplicaciones Usuario - 6817870, 6817871, 6818380 /Sun Microsystems - 1/21/2010 - Vulnerabilidad de Seguridad en PostgreSQL podría provocar una situación de Denegación de Servicio.
- Aplicaciones Usuario - 6854303 /Sun Microsystems - 1/21/2010 - Overflow de Buffer y de cálculo entero en el Entorno de ejecución de Java
- Aplicaciones Usuario - 6856923 /Sun Microsystems - 1/21/2010 - Vulnerabilidad de Seguridad en Sun Virtual Desktop Infrastructure
- Aplicaciones Usuario - 6738524 /Sun Microsystems - 1/21/2010 - Vulnerabilidad de seguridad en el entorno de ejecución de Java (Sistema de Audio)
- Sistemas Operativos - 6680381, 6653844 /Sun Microsystems - 1/21/2010 - Situación de "System Panic" al instalar Solaris 8 Migration Assistant 1.0
- Aplicaciones Usuario - 6863503 /Sun Microsystems - 1/21/2010 - Vulnerabilidad de Seguridad en el entorno de ejecución de Java podría permitir saltarse la autenticación
- Aplicaciones Usuario - 6792554 /Sun Microsystems - 1/21/2010 - Vulnerabilidades de Overflow de Buffer y de cálculo entero en el entorno de ejecución de Java podrían permitir la escalada de privilegios.
- Aplicaciones Usuario - 6497740 /Sun Microsystems - 1/21/2010 - Vulnerabilidad de Seguridad en el entorno de ejecución de Java al procesar llaves públicas RSA
- Aplicaciones Usuario - 6823373 /Sun Microsystems - 1/21/2010 - Overflow de enteros en el entorno de ejecución de Java
- Aplicaciones Usuario - 6880677, 6899624 /Sun Microsystems - 1/21/2010 - Vulnerabilidad de seguridad en los certificados SSL de Mozilla Thunderbird
- Aplicaciones Usuario - 4968715 /Sun Microsystems - 1/25/2010 - Los servicios remotos NetConnect Proxy podría ser susceptible a una pérdida de datos durante una transferencia
- Aplicaciones Usuario - 6683220 /Sun Microsystems - 1/25/2010 - Vulnerabilidad de Cross Site Scripting en el servidor de mensajería "Sun Java Messaging Server"

- **Sistemas Operativos - SUSE-SR:2010:001 - 1/19/2010 - Resumen de vulnerabilidades se seguridad en SUSE**
- **Sistemas Operativos - MAC-2010-ENE - 1/23/2010 - Varias vulnerabilidades en Mac OS**
- **Aplicaciones Usuario - APSB10-03 - 1/19/2010 - Actualización de seguridad disponible para Shockwave Player**
- **Aplicaciones Usuario - MS10-002 – Crítico - 1/21/2010 - Actualización de seguridad acumulativa para Internet Explorer (978207)**
- **Sistemas Operativos - VMSA-2010-0002 - 1/29/2010 - VMware vCenter update release addresses multiple security issues in Java JRE**

2. Boletín Detallado Vulnerabilidades

Aplicaciones Usuario - Fallo en la reconfiguración dinámica de Sun StorageTek VM/HSC

Fecha: 1/18/2010

Descripción:

Los clientes que utilicen Sun StorageTek no podrán acceder correctamente a sus SL3000 LSMs o añadir nuevo hardware a sus SL8500 LSM.

De forma adicional, adicionalmente, si el espacio de direcciones del VM/HSC se sature, VM/HSC requerirá un reinicio.

Productos Afectados:

Sun StorageTek VM/HSC 6.1 with PTF L1H151B applied

Sun StorageTek VM/HSC 6.2 with PTF L1H153D applied

Notas:

Todavía no se ha publicado una solución para el problema.

Las actualizaciones que se publicarán en breve son las siguientes:

VM/HSC 6.1 (SMS6100) - PTF L1H15FF

VM/HSC 6.2 (SMS6200) - PTF L1H15FH

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-275670-1>

CVEs:

Sistemas Operativos - Varias Vulnerabilidades en Solaris relacionadas con TCP podrían provocar condiciones de Denegación del Servicio

Fecha: 1/19/2010

Descripción:

Varias vulnerabilidades presentes en la implementación TCP de Solaris podría permitir a un usuario remoto privilegiado causar situaciones de Denegación de Servicio.

Productos Afectados:

SPARC Platform

Solaris 8

Solaris 9

Solaris 10

OpenSolaris based upon builds snv_01 through snv_130

x86 Platform

Solaris 8

Solaris 9

Solaris 10

OpenSolaris based upon builds snv_01 through snv_130

Notas:

SPARC Platform

OpenSolaris based upon builds snv_131 or later

x86 Platform

OpenSolaris based upon builds snv_131 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-267088-1>

CVEs:

CVE-2008-4609

Aplicaciones Usuario - Vulnerabilidad de Cross Site Scripting en el Servidor de Mensajes de Java

Fecha: 1/20/2010

Descripción:

Una vulnerabilidad de Cross Site Scripting en el Servidor de mensajes de Java podría permitir a un usuario remoto sin privilegios ejecutar código Javascript arbitrario en el navegador de un usuario.

Productos Afectados:

SPARC Platform

Sun Java System Messaging Server 6.2 and 6.3 (for Solaris 9 and Solaris 10) without patch 120228-29

Sun Java System Messaging Server 6.3 (64-bit Solaris) without patch 126479-10

x86 Platform

Sun Java System Messaging Server 6.2 and 6.3 (for Solaris 9 and Solaris 10) without patch 120229-29

Sun Java System Messaging Server 6.3 (64-bit) without patch 126480-10

Linux Platform

Sun Java System Messaging Server 6.2 and 6.3 (for RHEL 3 and RHEL 4) without patch 120230-29

Notas:

Solución:

Instalar los siguientes parches:

This issue is addressed in the following releases:

SPARC Platform

Sun Java System Messaging Server 6.2 and 6.3 (for Solaris 9 and Solaris 10) with patch 120228-29 or later

Sun Java System Messaging Server 6.3 (64-bit Solaris) with patch 126479-10 or later

x86 Platform

Sun Java System Messaging Server 6.2 and 6.3 (for Solaris 9 and Solaris 10) with patch 120229-29 or later

Sun Java System Messaging Server 6.3 (64-bit) with patch 126480-10 or later

Linux Platform

Sun Java System Messaging Server 6.2 and 6.3 (for RHEL 3 and RHEL 4) with patch 120230-29 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-242186-1>

CVEs:

Aplicaciones Usuario - Fallo en los comandos de reserva persistente

Fecha: 1/20/2010

Descripción:

Comandos de reserva persistente que se procesen lentamente en los Arrays de Sun Storagetek podrían producir pérdida de datos y Timeouts en el acceso a los sistemas de ficheros.

Productos Afectados:

Sun StorageTek 6140 Array running firmware without 06.60.11.10 (maintenance update) or 07.10.25.10 (feature update) or later firmware

Sun StorageTek 6540 Array running firmware without 06.60.11.10 (maintenance update) or 07.10.25.10 (feature update) or later firmware

Sun StorageTek Flexline 380 Array without 06.60.11.20 or 07.10.25.10 or later firmware

Notas:

Solución:

Seguir las indicaciones siguientes:

For 6140, 6540, and Flexline 380 arrays staying with the 06.xx firmware

6.60.11.10 is bundled with Sun StorageTek Common Array Manager(CAM) 6.1.0 or later:

CAM can be downloaded from

<http://www.sun.com/downloads> or

<http://www.sun.com/download/index.jsp?tab=2#S>

For 6140, 6540, and Flexline 380 arrays using Sun StorageTek SANtricity, customers wishing to get firmware 06.60.11.10 or later

Please contact Sun Support for the firmware release bundle. You will also need to get a new copy of SANtricity 10.10. Please order it from: https://www2.sun.de/dct/forms/reg_us_1508_643_0.jsp

For 6140, 6540, and Flexline 380 arrays going to the 07.10 firmware feature release

07.10.25.10 firmware is a feature release and requires a service call for an upgrade. It is not bundled with CAM or SANtricity.

CAM 6.1.0 or later is required

SANtricity 10.10 or later is required

Please contact Sun Support if you require the 07.10 feature release update.

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-231801-1>

CVEs:

Aplicaciones Usuario - Vulnerabilidad de Seguridad en PostgreSQL podría provocar una situación de Denegación de Servicio.

Fecha: 1/21/2010

Descripción:

Una vulnerabilidad de seguridad que afecta al software PostgreSQL podría permitir a usuarios no autenticados causar una Denegación del Servicio (DoS) en el servidor PostgreSQL.

Productos Afectados:

SPARC Platform

Solaris 10 PostgreSQL 8.1 without patch 123590-10

Solaris 10 PostgreSQL 8.2 without patch 136998-06

Solaris 10 PostgreSQL 8.3 without patch 138826-04

OpenSolaris PostgreSQL 8.1 based upon builds snv_01 through snv_109

OpenSolaris PostgreSQL 8.2 based upon builds snv_81 through snv_111

OpenSolaris PostgreSQL 8.3 based upon builds snv_87 through snv_111

x86 Platform

Solaris 10 PostgreSQL 8.1 without patch 123591-10

Solaris 10 PostgreSQL 8.2 without patch 136999-06

Solaris 10 PostgreSQL 8.3 without patch 138827-04

OpenSolaris PostgreSQL 8.1 based upon builds snv_01 through snv_109

OpenSolaris PostgreSQL 8.2 based upon builds snv_81 through snv_111

OpenSolaris PostgreSQL 8.3 based upon builds snv_87 through snv_111

Notas:

Solución:

Instalar los siguientes parches:

SPARC Platform

Solaris 10 PostgreSQL 8.1 with patch 123590-10 or later

Solaris 10 PostgreSQL 8.2 with patch 136998-06 or later

Solaris 10 PostgreSQL 8.3 with patch 138826-04 or later

OpenSolaris PostgreSQL 8.2 based upon builds snv_111a or later

OpenSolaris PostgreSQL 8.3 based upon builds snv_111a or later

x86 Platform

Solaris 10 PostgreSQL 8.1 with patch 123591-10 or later

Solaris 10 PostgreSQL 8.2 with patch 136999-06 or later

Solaris 10 PostgreSQL 8.3 with patch 138827-04 or later

OpenSolaris PostgreSQL 8.2 based upon builds snv_111a or later

OpenSolaris PostgreSQL 8.3 based upon builds snv_111a or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-258808-1>

CVEs:

Aplicaciones Usuario - Overflow de Buffer y de cálculo entero en el Entorno de ejecución de Java

Fecha: 1/21/2010

Descripción:

Varias vulnerabilidades de overflow de buffer y de cálculo de enteros en el Entorno de ejecución de java, producidas al procesar audio y archivos de imagen podrían permitir a un applet malicioso o a la aplicación Java Web Start realizar una escalada de privilegios.

Productos Afectados:

Java SE for Windows, Solaris, and Linux:

JDK and JRE 6 Update 16 and earlier

JDK and JRE 5.0 Update 21 and earlier

Java SE for Solaris:

SDK and JRE 1.4.2_23 and earlier

Java SE for Windows:

SDK and JRE 1.3.1_26 and earlier

Java SE for Business for Windows, Solaris and Linux:

JDK and JRE 6 Update 16 and earlier

JDK and JRE 5.0 Update 21 and earlier

SDK and JRE 1.4.2_23 and earlier

The issues described in CR 6874643 and 6862968 can occur in the following releases:

Java SE for Windows, Solaris, and Linux:

JDK and JRE 6 Update 16 and earlier

JDK and JRE 5.0 Update 21 and earlier

Java SE for Solaris:

SDK and JRE 1.4.2_23 and earlier

Java SE for Business for Windows, Solaris and Linux:

JDK and JRE 6 Update 16 and earlier

JDK and JRE 5.0 Update 21 and earlier

SDK and JRE 1.4.2_23 and earlier

Notas:

Solución: Instalar los siguientes parches:

Java SE for Windows, Solaris, and Linux:

JDK and JRE 6 Update 17 or later

JDK and JRE 5.0 Update 22 or later

Java SE for Solaris:

SDK and JRE 1.4.2_24 or later

Java SE for Windows:

SDK and JRE 1.3.1_27 or later

Java SE for Business for Windows, Solaris and Linux:

JDK and JRE 6 Update 17 or later

JDK and JRE 5.0 Update 22 or later

SDK and JRE 1.4.2_24 or later

The issues described in CR 6874643 and 6862968 are addressed in the following releases:

Java SE for Windows, Solaris, and Linux:

JDK and JRE 6 Update 17 or later

JDK and JRE 5.0 Update 22 or later

Java SE for Solaris:

SDK and JRE 1.4.2_24 or later

Java SE for Business for Windows, Solaris and Linux:

JDK and JRE 6 Update 17 or later

JDK and JRE 5.0 Update 22 or later

SDK and JRE 1.4.2_24 or later

Java SE releases are available at:

JDK and JRE 6 Update 17:

<http://java.sun.com/javase/downloads/index.jsp>

JRE 6 Update 17:

<http://java.com/>

Through the Java Update tool for Microsoft Windows users

JDK 6 Update 17 for Solaris is available in the following patches:

Java SE 6: update 17 (as delivered in patch 125136-18)

Java SE 6: update 17 (as delivered in patch 125137-18 (64bit))

Java SE 6_x86: update 17 (as delivered in patch 125138-18)

Java SE 6_x86: update 17 (as delivered in patch 125139-18 (64bit))

Note: After release it was discovered that the following patches do not install:

125136-18 125137-18 125138-18 125139-18 These are harmless because they do not install at all.

To resolve the issue described in this Sun Alert, please use the next revision of these patches:

125136-19 125137-19 125138-19 125139-19 JDK and JRE 5.0 Update 22:

http://java.sun.com/javase/downloads/index_jdk5.jsp

JDK 5.0 Update 22 for Solaris is available in the following patches:

J2SE 5.0: update 22 (as delivered in patch 118666-24)

J2SE 5.0: update 22 (as delivered in patch 118667-24 (64bit))

J2SE 5.0_x86: update 22 (as delivered in patch 118668-24)

J2SE 5.0_x86: update 22 (as delivered in patch 118669-24 (64bit))

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-270474-1>

CVEs:

Aplicaciones Usuario - Vulnerabilidad de Seguridad en Sun Virtual Desktop Infrastructure

Fecha: 1/21/2010

Descripción:

Una vulnerabilidad de seguridad en Sun Virtual Desktop Infrastructure (VDI) Software 3.0 podría permitir a un usuario remoto con privilegios ser capaz de ver las peticiones LDAP de los datos de configuración de VDI.

Productos Afectados:

SPARC Platform

Sun VDI Software 3.0 (for Solaris 10) without patch 141481-02
x86 Platform

Sun VDI Software 3.0 (for Solaris 10) without patch 141482-02

Notas:

Solución: Instalar los siguientes parches:

SPARC Platform

Sun VDI Software 3.0 (for Solaris 10) with patch 141481-02 or later

x86 Platform

Sun VDI Software 3.0 (for Solaris 10) with patch 141482-02 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-265488-1>

CVEs:

Aplicaciones Usuario - Vulnerabilidad de seguridad en el entorno de ejecución de Java (Sistema de Audio)

Fecha: 1/21/2010

Descripción:

Esta vulnerabilidad de seguridad en el Sistema de Audio del entorno de ejecución de Java podría permitir el acceso a las propiedades del sistema.

Productos Afectados:

JDK and JRE 6 Update 14 and earlier

JDK and JRE 5.0 Update 19 and earlier

Notas:

JDK and JRE 6 Update 15 or later

JDK and JRE 5.0 Update 20 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-263408-1>

CVEs:

Sistemas Operativos - Situación de "System Panic" al instalar Solaris 8 Migration Assistant 1.0

Fecha: 1/21/2010

Descripción:

Bjo determinadas condiciones, instalar Solaris 8 Migration Assistant 1.0 en Solaris 10 puede causar una situación de "System Panic".

Productos Afectados:

SPARC Platform

Solaris 10 with Patch 127111-05 or later and without patch 128548-05

Notas:

Instalar el siguiente parche:

Solaris 10 with patch 128548-05 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-236661-1>

CVEs:

Aplicaciones Usuario - Vulnerabilidad de Seguridad en el entorno de ejecución de Java podría permitir saltarse la autenticación

Fecha: 1/21/2010

Descripción:

Una vulnerabilidad de seguridad en el entorno de ejecución de Java al verificar las "HMAC digests" podría permitir saltarse la autenticación. Esto podría permitir a un usuario crear una firma digital aceptada como válida.

Las aplicaciones que validan las firmas digitales basadas en HMAC podrían ser vulnerables a este tipo de ataques.

Productos Afectados:

Java SE for Windows, Solaris, and Linux:

JDK and JRE 6 Update 16 and earlier

JDK and JRE 5.0 Update 21 and earlier

Java SE for Solaris:

SDK and JRE 1.4.2_23 and earlier

Java SE for Windows:

SDK and JRE 1.3.1_26 and earlier

Java SE for Business for Windows, Solaris and Linux:

JDK and JRE 6 Update 16 and earlier

JDK and JRE 5.0 Update 21 and earlier

SDK and JRE 1.4.2_23 and earlier

Notas:

Solución: Instalar los siguientes parches:

Java SE for Windows, Solaris, and Linux:

JDK and JRE 6 Update 17 or later

JDK and JRE 5.0 Update 22 or later

Java SE for Solaris:

SDK and JRE 1.4.2_24 or later

Java SE for Windows:

SDK and JRE 1.3.1_27 or later

Java SE for Business for Windows, Solaris and Linux:

JDK and JRE 6 Update 17 or later

JDK and JRE 5.0 Update 22 or later

SDK and JRE 1.4.2_24 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-270475-1>

CVEs:

Aplicaciones Usuario - Vulnerabilidades de Overflow de Buffer y de cálculo entero en el entorno de ejecución de Java podrían permitir la escalada de privilegios.

Fecha: 1/21/2010

Descripción:

Varias vulnerabilidades de Overflow de Buffer y de cálculo de enteros en el entorno de ejecución de Java al utilizar el programa unpack200 JAR podría permitir escalar privilegios mediante applet malicioso o el programa Java Web Start.

Productos Afectados:

JDK and JRE 5.0 Update 17 and earlier

JDK and JRE 6 Update 12 and earlier

Notas:

Solución: Instalar los siguientes parches:

JDK and JRE 5.0 Update 18 or later

JDK and JRE 6 Update 13 or later

Java SE releases are available at:

JDK and JRE 6 Update 13:

<http://java.sun.com/javase/downloads/index.jsp>

JRE 6 Update 13:

<http://java.com/>

Through the Java Update tool for Microsoft Windows users

JDK 6 Update 13 for Solaris is available in the following patches:

Java SE 6: update 13 (as delivered in patch 125136-14)

Java SE 6: update 13 (as delivered in patch 125137-14 (64bit))

Java SE 6_x86: update 13 (as delivered in patch 125138-14)

Java SE 6_x86: update 13 (as delivered in patch 125139-14 (64bit))

JDK and JRE 5.0 Update 18:

http://java.sun.com/javase/downloads/index_jdk5.jsp

JDK 5.0 Update 18 for Solaris is available in the following patches:

J2SE 5.0: update 18 (as delivered in patch 118666-19)

J2SE 5.0: update 18 (as delivered in patch 118667-19 (64bit))

J2SE 5.0_x86: update 18 (as delivered in patch 118668-19)

J2SE 5.0_x86: update 18 (as delivered in patch 118669-19 (64bit))

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-254570-1>

CVEs:

Aplicaciones Usuario - Vulnerabilidad de Seguridad en el entorno de ejecución de Java al procesar llaves públicas RSA

Fecha: 1/21/2010

Descripción:

Una vulnerabilidad de seguridad en el entorno de ejecución de Java al procesar determinadas llaves RSA públicas podría provocar que JRE consumiera una cantidad excesiva de CPU, dando como resultado una situación de Denegación de Servicio.

Productos Afectados:

JDK and JRE 6 Update 10 or earlier

JDK and JRE 5.0 Update 16 or earlier

Notas:

Solución: Instalar los siguientes parches:

JDK and JRE 6 Update 11 or later

JDK and JRE 5.0 Update 17 or later

Java SE releases are available at:

JDK 6 Update 11:

<http://java.sun.com/javase/downloads/index.jsp>

JRE 6 Update 11:

<http://java.sun.com/javase/downloads/index.jsp>

<http://java.com/>

and through the Java Update tool for Microsoft Windows users.

JDK 6 Update 11 is also available for Solaris in the following patches:

Java SE 6: update 11 (as delivered in patch 125136-12)

Java SE 6: update 11 (as delivered in patch 125137-12 (64bit))

Java SE 6_x86: update 11 (as delivered in patch 125138-12)

Java SE 6_x86: update 11 (as delivered in patch 125139-12 (64bit))

JDK and JRE 5.0 Update 17:

http://java.sun.com/javase/downloads/index_jdk5.jsp

JDK 5.0 Update 17 is also available for Solaris in the following patches:

J2SE 5.0: update 17 (as delivered in patch 118666-18)

J2SE 5.0: update 17 (as delivered in patch 118667-18 (64bit))

J2SE 5.0_x86: update 17 (as delivered in patch 118668-18)

J2SE 5.0_x86: update 17 (as delivered in patch 118669-18 (64bit))

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-246286-1>

CVEs:

Aplicaciones Usuario - Overflow de enteros en el entorno de ejecución de Java

Fecha: 1/21/2010

Descripción:

Una vulnerabilidad de cálculo de enteros en el entorno de ejecución de Java cuando se parsea una imagen JPEG podría permitir a una aplicación Web de Java maliciosa realizar una escalada de privilegios.

Productos Afectados:

JDK and JRE 6 Update 14 and earlier

Notas:

Solución: Instalar los siguientes parches:

This issue is addressed in the following Java SE and Java SE for Business releases for Windows, Solaris, and Linux:

JDK and JRE 6 Update 15 or later

Java SE releases are available at:

JDK and JRE 6 Update 15:

<http://java.sun.com/javase/downloads/index.jsp>

JRE 6 Update 15:

<http://java.com/>

Through the Java Update tool for Microsoft Windows users

JDK 6 Update 15 for Solaris is available in the following patches:

Java SE 6: update 15 (as delivered in patch 125136-16)

Java SE 6: update 15 (as delivered in patch 125137-16 (64bit))

Java SE 6_x86: update 15 (as delivered in patch 125138-16)

Java SE 6_x86: update 15 (as delivered in patch 125139-16 (64bit))

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-263428-1>

CVEs:

Aplicaciones Usuario - Vulnerabilidad de seguridad en los certificados SSL de Mozilla Thunderbird

Fecha: 1/21/2010

Descripción:

Varias vulnerabilidades en Thunderbird que afectan al manejo de certificados de servidor podrían permitir a servidores SSL remotos con certificados de servidor falseados comprometer la comunicación encriptada o causar una ejecución arbitraria de código con privilegios de un usuario de Thunderbird.

Productos Afectados:

SPARC platform

Solaris 10 without patch 125541-06

OpenSolaris based upon builds snv_48 through snv_124

x86 Platform

Solaris 10 without patch 125542-06

OpenSolaris based upon builds snv_48 through snv_124

Notas:

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-269468-1>

CVEs:

Aplicaciones Usuario - Los servicios remotos NetConnect Proxy podría ser susceptible a una pérdida de datos durante una transferencia

Fecha: 1/25/2010

Descripción:

La configuración de los datos del Service Tracker podría perder confiabilidad en la Administración del sistema de Disponibilidad de Sun. Si los servicios remotos de SUN ejecutan una versión del proxy anterior a la 1.0.4, los datos del Service Tracker no estarán disponibles en la Base de Datos del Sistema de Administración de Disponibilidad de Sun

Productos Afectados:

SPARC Platform

SRS NetConnect version prior to 3.0.4 (with proxy version prior to 1.0.4)

Notas:

Para solucionar el problema, se deberán seguir las instrucciones indicadas en la sección "Software Undates" del capítulo 8 de la guía "NetConnect Customer Operations Guide".

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-200374-1>

CVEs:

Aplicaciones Usuario - Vulnerabilidad de Cross Site Scripting en el servidor de mensajería "Sun Java Messaging Server"

Fecha: 1/25/2010

Descripción:

Existe una vulnerabilidad de Cross Site Scripting en el Servidor "Sun Java System Messaging" Server que podría permitir a un usuario remoto sin privilegios ejecutar código Javascript en el navegador de un usuario.

Productos Afectados:

SPARC Platform

Sun Java System Messaging Server 6.2 and 6.3 (for Solaris 9 and Solaris 10) without patch 120228-29

Sun Java System Messaging Server 6.3 (64-bit Solaris) without patch 126479-10

x86 Platform

Sun Java System Messaging Server 6.2 and 6.3 (for Solaris 9 and Solaris 10) without patch 120229-29

Sun Java System Messaging Server 6.3 (64-bit) without patch 126480-10

Linux Platform

Sun Java System Messaging Server 6.2 and 6.3 (for RHEL 3 and RHEL 4) without patch 120230-29

Notas:

Solución: Instalar los parches siguientes:

SPARC Platform

Sun Java System Messaging Server 6.2 and 6.3 (for Solaris 9 and Solaris 10) without patch 120228-29

Sun Java System Messaging Server 6.3 (64-bit Solaris) without patch 126479-10

x86 Platform

SPARC Platform

Sun Java System Messaging Server 6.2 and 6.3 (for Solaris 9 and Solaris 10) with patch 120228-29 or later

Sun Java System Messaging Server 6.3 (64-bit Solaris) with patch 126479-10 or later

x86 Platform

Sun Java System Messaging Server 6.2 and 6.3 (for Solaris 9 and Solaris 10) with patch 120229-29 or later

Sun Java System Messaging Server 6.3 (64-bit) with patch 126480-10 or later
Linux Platform

Sun Java System Messaging Server 6.2 and 6.3 (for RHEL 3 and RHEL 4) with patch 120230-29 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-242186-1>

CVEs:

Sistemas Operativos - Resumen de vulnerabilidades de seguridad en SUSE

Fecha: 1/19/2010

Descripción:

Se han publicado parches que solucionan vulnerabilidades relacionadas con:

- expat
- postfix
- phpMyAdmin
- postgresql
- dovecot12
- msmtpl

A continuación, se incluye una breve descripción de cada problema de seguridad encontrado:

-expat: Errores al parsear archivos xml.

-postfix: Accidentalmente, postfix se queda escuchando en todos los interfaces de red.

-phpMyAdmin: La utilización de unserialize() podría permitir una ejecución remota de código.

-postgresql: Un usuario autenticado, sin privilegios puede crear una tabla que referencie a funciones con contenido malicioso.

-Dovecot12: Dovecot crea el directorio base_dir en el modo 0777, permitiendo el acceso y modificación a todos los usuarios locales.

-msmtpl: No se trata correctamente el carácter '\0' del nombre de dominio de los certificados SSL.

Productos Afectados:

expat: SLES9, SLE10-SP2, SLE10-SP3, SLE11, openSUSE 11.0-11.2

postfix: SLE10-SP3

phpMyAdmin: openSUSE 11.0

postgresql: SLES9, SLE10-SP2, SLE10-SP3, SLE11, openSUSE 11.0-11.2

dovecot: openSUSE 11.2

msmtpl: openSUSE 11.0-11.2

Notas:

Se han publicado soluciones que solventan todos y cada uno de los problemas descritos.

Referencias en la web:

http://www.novell.com/linux/security/advisories/2010_1_sr.html

CVEs:

CVE-2008-7251 CVE-2008-7252 CVE-2009-3560 CVE-2009-3897 CVE-2009-3942 CVE-2009-4034 CVE-2009-4136 CVE-2009-4605 CVE-2010-0230

Sistemas Operativos - Varias vulnerabilidades en Mac OS

Fecha: 1/23/2010

Descripción:

CoreAudio

CVE-ID: CVE-2010-0036

Disponible para: Mac OS X v10.5.8, Mac OS X Server v10.5.8, Mac OS X v10.6.2, Mac OS X Server v10.6.2

Impacto: la apertura de un archivo de audio mp4 creado con fines malintencionados puede provocar la finalización inesperada de la aplicación o la ejecución de código arbitrario

Descripción: se produce un desbordamiento del búfer en el manejo de archivos de audio mp4. La reproducción de un archivo de audio mp4 creado con fines malintencionados puede provocar la finalización inesperada de la aplicación o la ejecución de código arbitrario. Este problema se resuelve mejorando la comprobación de los límites. Gracias a Tobias Klein de trapkit.de por informar de este problema.

CUPS

CVE-ID: CVE-2009-3553

Disponible para: Mac OS X v10.5.8, Mac OS X Server v10.5.8, Mac OS X v10.6.2, Mac OS X Server v10.6.2

Impacto: un atacante remoto puede provocar la finalización inesperada de la aplicación cups

Descripción: existe un problema de uso después de liberación en cups. Un atacante puede causar una denegación del servicio remoto mediante una solicitud de número de trabajos pendientes de impresión creada con fines malintencionados. Esto se mitiga mediante el reinicio de cups tras su finalización. Este problema se resuelve mejorando el seguimiento del uso de la conexión.

Plug-in de Flash Player

CVE-ID: CVE-2009-3794, CVE-2009-3796, CVE-2009-3797, CVE-2009-3798, CVE-2009-3799, CVE-2009-3800, CVE-2009-3951

Disponible para: Mac OS X v10.5.8, Mac OS X Server v10.5.8, Mac OS X v10.6.2, Mac OS X Server v10.6.2

Impacto: múltiples vulnerabilidades en el plug-in de Adobe Flash Player

Descripción: existen múltiples problemas con el plug-in de Adobe Flash Player. El más grave de ellos puede provocar la ejecución de código arbitrario cuando se visualiza un sitio web creado de manera malintencionada. Este problema se resuelve mediante la actualización del plug-in de Flash Player a la versión 10.0.42. Hay más información disponible en el sitio web de Adobe en <http://www.adobe.com/es/support/security/bulletins/apsb09-19.html>. Gracias a un investigador anónimo y a Damian Put en colaboración con TippingPoints Zero Day Initiative, a Bing Liu del equipo de investigación de FortiGuard Global Security de Fortinet, a Will Dormann del CERT, a Manuel Caballero y a Microsoft Vulnerability Research (MSVR).

ImageIO

CVE-ID: CVE-2009-2285

Disponible para: Mac OS X v10.5.8, Mac OS X Server v10.5.8

Impacto: la visualización de una imagen TIFF creada con fines malintencionados puede provocar la finalización inesperada de una aplicación o la ejecución de código arbitrario

Descripción: existe un desbordamiento del búfer de pila en el manejo de imágenes TIFF por parte de ImageIO. La visualización de una imagen TIFF creada con fines malintencionados puede provocar la finalización inesperada de una aplicación o la ejecución de código arbitrario. Este problema se resuelve mediante la mejora de la comprobación de límites. Para los sistemas que utilizan Mac OS X v10.6, este problema se resuelve en Mac OS X v10.6.2.

Image RAW

CVE-ID: CVE-2010-0037

Disponible para: Mac OS X v10.5.8, Mac OS X Server v10.5.8, Mac OS X v10.6.2, Mac OS X Server v10.6.2

Impacto: la visualización de una imagen DNG creada con fines malintencionados puede provocar la finalización inesperada de la aplicación o la ejecución de código arbitrario

Descripción: se produce un desbordamiento en el búfer cuando se procesan imágenes DNG en formato RAW. La visualización de una imagen DNG creada con fines malintencionados puede provocar la finalización inesperada de la aplicación o la ejecución de código arbitrario. Este problema se resuelve mejorando la comprobación de los límites. Gracias a Jason Carr, de los Servicios de computación de Carnegie Mellon University, por informar acerca de este problema.

OpenSSL

CVE-ID: CVE-2009-3555

Disponible para: Mac OS X v10.5.8, Mac OS X Server v10.5.8, Mac OS X v10.6.2, Mac OS X Server v10.6.2

Impacto: un atacante con una posición de red privilegiada puede capturar datos o cambiar las operaciones que se realizan en sesiones protegidas por SSL

Descripción: existe una vulnerabilidad de interceptación en los protocolos SSL y TLS. Hay más información disponible en <http://www.phonefactor.com/sslgap>. Dentro de IETF hay un cambio en curso en la renegociación del protocolo. Como medida de seguridad preventiva, esta actualización inhabilita la renegociación en OpenSSL. Este problema no afecta a los servicios que utilizan Secure Transport ya que no requiere la renegociación. Gracias a Steve Dispensa y Marsh Ray de PhoneFactor, Inc. por informar acerca de este problema.

Productos Afectados:

Mac OS X v10.5.8, Mac OS X Server v10.5.8, Mac OS X v10.6.2, Mac OS X Server v10.6.2

Notas:

Referencias en la web:

CVEs:

CVE-2010-0036

Aplicaciones Usuario - Actualización de seguridad disponible para Shockwave Player

Fecha: 1/19/2010

Descripción:

Se han identificado vulnerabilidades importantes en Adobe Shockwave Player 11.5.2.602 y en versiones anteriores en los sistemas operativos Windows y Macintosh. Un intruso podría aprovecharse de estas vulnerabilidades para ejecutar un código malicioso en el sistema afectado. Adobe ha proporcionado una solución para las vulnerabilidades indicadas. Se recomienda que los usuarios actualicen sus instalaciones a la última versión siguiendo las instrucciones que se ofrecen a continuación.

Productos Afectados:

Shockwave Player 11.5.2.602 y versiones anteriores para Windows y Macintosh

Notas:

Adobe recomienda que los usuarios de Shockwave Player desinstalen la versión 11.5.2.602 de Shockwave y versiones anteriores de sus sistemas, reinicien los equipos e instalen la versión 11.5.6.606 de Shockwave, que está disponible aquí: <http://get.adobe.com/es/shockwave/>

Referencias en la web:

<http://www.adobe.com/es/support/security/bulletins/apsb10-03.html>

<http://cve.mitre.org/>

CVEs:

CVE-2009-4002, CVE-2009-4003

Aplicaciones Usuario - Actualización de seguridad acumulativa para Internet Explorer (978207)

Fecha: 1/21/2010

Descripción:

Esta actualización de seguridad resuelve siete vulnerabilidades de las que se ha informado de forma privada y una vulnerabilidad de la que se ha informado de forma pública en Internet Explorer. La más grave de las vulnerabilidades podría permitir la ejecución remota de código si un usuario de Internet Explorer visita una página web especialmente diseñada. Por tanto, los usuarios cuyas cuentas estén configuradas con pocos derechos de usuario en el sistema correrían un riesgo menor que aquellos que cuenten con derechos de usuario administrativos.

Productos Afectados:

Esta actualización de seguridad se considera crítica para todas las versiones compatibles de Internet Explorer: Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 6 Service Pack 1, Internet Explorer 7 e Internet Explorer 8 (excepto Internet Explorer 6 para las ediciones compatibles de Windows Server 2003). Para Internet Explorer 6 para las ediciones compatibles de Windows Server 2003 tal como se indica, esta actualización se considera moderada. Para obtener más información, consulte la subsección Software afectado y no afectado, en esta sección.

Notas:

La actualización de seguridad corrige estas vulnerabilidades al modificar la forma en que Internet Explorer trata los objetos en memoria, valida los parámetros de entrada y filtra los atributos HTML.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-002.msp>

<http://cve.mitre.org/>

CVEs:

CVE-2009-4074, CVE-2010-0027, CVE-2010-0244, CVE-2010-0245, CVE-2010-0246, CVE-2010-0247, CVE-2010-0248, CVE-2010-0249

Sistemas Operativos - VMware vCenter update release addresses multiple security issues in Java JRE

Fecha: 1/29/2010

Descripción:

Múltiples vulnerabilidades de seguridad en versiones anteriores a JRE 1.5.0_22

Productos Afectados:

Virtual Center 2.5 before Update 6

Notas:

Para solucionar la vulnerabilidad, descargar:

<http://downloads.vmware.com/download/download.do?downloadGroup=VC250U6>

Referencias en la web:

<http://www.vmware.com/security/advisories/VMSA-2010-0002.html>

<http://cve.mitre.org/>

CVEs:

CVE-2009-1093 CVE-2009-1094 CVE-2009-1095 CVE-2009-1096 CVE-2009-1097 CVE-2009-1098 CVE-2009-1099 CVE-2009-1100 CVE-2009-1101 CVE-2009-1102 CVE-2009-1103 CVE-2009-1104 CVE-2009-1105 CVE-2009-1106 CVE-2009-1107 CVE-2009-2625 CVE-2009-2670 CVE-2009-2671 CVE-2009-2672 CVE-2009-2673 CVE-2009-2675 CVE-2009-2676 CVE-2009-2716 CVE-2009-2718 CVE-2009-2719 CVE-2009-2720 CVE-2009-2721 CVE-2009-2722 CVE-2009-2723 CVE-2009-2724 CVE-2009-3728 CVE-2009-3729 CVE-2009-3864 CVE-2009-3865 CVE-2009-3866 CVE-2009-3867 CVE-2009-3868 CVE-2009-3869 CVE-2009-3871 CVE-2009-3872 CVE-2009-3873 CVE-2009-3874 CVE-2009-3875 CVE-2009-3876 CVE-2009-3877 CVE-2009-3879 CVE-2009-3880 CVE-2009-3881 CVE-2009-3882 CVE-2009-3883 CVE-2009-3884 CVE-2009-3886 CVE-2009-3885

