

BOLETÍN DE VULNERABILIDADES
ÁUDEA, SEGURIDAD DE LA INFORMACIÓN
15 DE ABRIL 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 - MFSA 2010-25 Crítico - 4/1/2010 - Reutilización de objeto liberado debido a confusión de alcance
- Sistemas Operativos - MS10-019 - Crítico - 4/13/2010 - Vulnerabilidades en Windows podrían permitir la ejecución remota de código (981210)
- Sistemas Operativos - MS10-020 - Crítico - 4/13/2010 - Vulnerabilidades en el cliente SMB podrían permitir la ejecución remota de código (980232)
- Sistemas Operativos - MS10-021 - Importante - 4/13/2010 - Vulnerabilidades del kernel de Windows podrían permitir la elevación de privilegios (979683)
- Sistemas Operativos - MS10-022 - Importante - 4/13/2010 - Una vulnerabilidad en el motor de secuencias de comandos de VBScript podría permitir la ejecución remota de código (981169)
- Sistemas Operativos - MS10-023 - Importante - 4/13/2010 - Una vulnerabilidad en Microsoft Office Publisher podría permitir la ejecución remota de código (981160)
- Sistemas Operativos - MS10-024 - Importante - 4/13/2010 - Vulnerabilidades en Microsoft Exchange y el servicio SMTP de Windows podrían permitir la denegación de servicio (981832)
- Sistemas Operativos - MS10-025 - Crítico - 4/13/2010 - Una vulnerabilidad en Servicios de Microsoft Windows Media podría permitir la ejecución remota de código (980858)
- Sistemas Operativos - MS10-026 - Crítico - 4/13/2010 - Una vulnerabilidad en los códecs MPEG Layer-3 de Microsoft podría permitir la ejecución remota de código (977816)
- Sistemas Operativos - MS10-027 - Crítico - 4/13/2010 - Una vulnerabilidad en el Reproductor de Windows Media podría permitir la ejecución remota de código (979402)
- Sistemas Operativos - MS10-028 - Importante - 4/13/2010 - Vulnerabilidades en Microsoft Visio podrían permitir la ejecución remota de código (980094)
- Sistemas Operativos - MS10-029 - Moderado - 4/13/2010 - Una vulnerabilidad en el componente ISATAP de Windows podría permitir la suplantación de personalidad (978338)
- Aplicaciones Usuario - 6872718, 6861920 /Sun Microsystems - 4/12/2010 - Alerta de Seguridad en el producto Sun Java System Access Manager
- Sistemas Operativos - 6343194 /Sun Microsystems - 4/12/2010 - Alerta de seguridad en "kernel component" de Solaris y OpenSolaris
- Aplicaciones Usuario - 6902029 /Sun Microsystems - 4/12/2010 - Vulnerabilidad en el Demonio NTP
- Aplicaciones Usuario - 6874719, 6843063 /Sun Microsystems - 4/12/2010 - Alerta de seguridad en el componente "Directory Server" de los productos Sun ONE Directory Server y Sun Java System Directory Server

- **Aplicaciones Usuario - 6906268 /Sun Microsystems - 4/15/2010 - Vulnerabilidad de seguridad en la utilidad "automake" de Solaris**
- **Sistemas Operativos - SUSE-SR:2010:008 - 4/7/2010 - Vulnerabilidades en el Kernel de SUSE**
- **Sistemas Operativos - SUSE-SR:2010:009 - 4/14/2010 - Vulnerabilidades en el Kernel de SUSE**
- **Sistemas Operativos - RHSA-2010:0342-01 - 4/6/2010 - Bug fix en el Kernel de Red Hat Linux**
- **Aplicaciones Usuario - RHSA-2010:0343-01 - 4/6/2010 - Actualización de krb5**
- **Bases de Datos - RHSA-2010:0347-01 - 4/13/2010 - Nuevos paquetes nss_db que solucionan varios problemas de seguridad**
- **Sistemas Operativos - RHSA-2010:0348-01 - 4/14/2010 - Actualización importante en kdbase**
- **Aplicaciones Usuario - RHSA-2010:0349-01 - 4/14/2010 - Actualización de seguridad en Acroread**
- **Bases de Datos - ORA April 2010 - 4/1/2010 - Oracle Critical Patch Update Advisory - April 2010**
- **Aplicaciones Usuario - CA20100406-01 - 4/6/2010 - Security Notice for CA Xosoft**
- **Sistemas Operativos - VMWARE VMSA-2010-0007.1 - 4/9/2010 - VMware Security Advisory**

2. Boletín Detallado Vulnerabilidades

Aplicaciones Usuario - Reutilización de objeto liberado debido a confusión de alcance

Fecha: 4/1/2010

Descripción:

Un fallo de corrupción de memoria que puede llevar a la ejecución de código ha sido reportada por el investigador Nils, de MWR InfoSecurity, durante el concurso "Pwn2Own 2010" patrocinado por "TippingPoint's Zero Day Initiative". Moviendo nodos DOM entre documentos Nils descubrió un caso en el que el nodo movido mantenía de forma incorrecta su antiguo alcance. Firefox utilizaría posteriormente este objeto liberado.

Productos Afectados:

Firefox

Notas:

Solucionado en Firefox 3.6.3

Referencias en la web:

<http://www.mozilla.org/security/announce/2010/mfsa2010-25.html>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1121>

CVEs:

CVE-2010-1121

Sistemas Operativos - Vulnerabilidades en Windows podrían permitir la ejecución remota de código (981210)

Fecha: 4/13/2010

Descripción:

Esta actualización de seguridad resuelve dos vulnerabilidades de las que se ha informado de forma privada en la comprobación de Authenticode de Windows que podría permitir la ejecución remota de código. Un atacante que aprovechara cualquiera de estas vulnerabilidades podría lograr el control completo de un sistema afectado. De esta forma, un intruso podría instalar programas; ver, cambiar o eliminar datos; o crear cuentas nuevas con todos los derechos de usuario.

Productos Afectados:

Esta actualización de seguridad se considera crítica para todas las versiones compatibles de Microsoft Windows.

Notas:

La actualización de seguridad corrige las vulnerabilidades al realizar operaciones de comprobación adicionales al firmar y al comprobar un archivo portable ejecutable o .CAB.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-019.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0486>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0487>

CVEs:

CVE-2010-0486, CVE-2010-0487

Sistemas Operativos - Vulnerabilidades en el cliente SMB podrían permitir la ejecución remota de código (980232)

Fecha: 4/13/2010

Descripción:

Esta actualización de seguridad resuelve una vulnerabilidad de la que se ha informado de forma pública y otras vulnerabilidades de las que se ha informado de forma privada en Microsoft Windows. Las vulnerabilidades podrían permitir la ejecución remota de código si un atacante ha enviado una respuesta SMB especialmente diseñada a una solicitud SMB iniciada por el cliente. Para aprovechar estas vulnerabilidades, un atacante debe convencer al usuario para que inicie una conexión SMB a un servidor SMB especialmente diseñado.

Productos Afectados:

Esta actualización de seguridad se considera crítica para todas las ediciones compatibles de Microsoft Windows.

Notas:

La actualización de seguridad corrige las vulnerabilidades al modificar la manera en que el cliente SMB trata las respuestas SMB, asigna memoria y valida campos en la respuesta SMB.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-020.msp>

<http://cve.mitre.org>

CVEs:

CVE-2009-3676, CVE-2010-0269, CVE-2010-0270, CVE-2010-0476, CVE-2010-0477

Sistemas Operativos - Vulnerabilidades del kernel de Windows podrían permitir la elevación de privilegios (979683)

Fecha: 4/13/2010

Descripción:

Esta actualización de seguridad resuelve varias vulnerabilidades de las que se ha informado de forma privada en Microsoft Windows. La más grave de estas vulnerabilidades podría permitir la elevación de privilegios si un atacante ha iniciado sesión localmente y ha ejecutado una aplicación especialmente diseñada. Para aprovechar esta vulnerabilidad, un atacante debe de tener unas credenciales de inicio de sesión válidas y ser capaz de aprovechar estas vulnerabilidades. Los usuarios anónimos o los usuarios remotos no pueden aprovechar estas vulnerabilidades.

Productos Afectados:

Esta actualización de seguridad se considera importante para todas las ediciones compatibles de Microsoft Windows 2000, Windows XP, Windows Server 2003 y la versión original de Windows Vista. Esta actualización de seguridad se considera moderada para todas las ediciones compatibles de Windows Vista Service Pack 1, Windows Vista Service Pack 2, Windows Server 2008, Windows 7 y Windows Server 2008 R2.

Notas:

La actualización de seguridad corrige las vulnerabilidades al modificar las validaciones, la creación de vínculos simbólicos, la resolución de rutas de acceso virtuales de las claves del Registro y el tratamiento de excepciones.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-021.msp>

<http://cve.mitre.org>

CVEs:

CVE-2010-0234, CVE-2010-0235, CVE-2010-0236, CVE-2010-0237, CVE-2010-0238, CVE-2010-0481, CVE-2010-0482, CVE-2010-0810

Sistemas Operativos - Una vulnerabilidad en el motor de secuencias de comandos de VBScript podría permitir la ejecución remota de código (981169)

Fecha: 4/13/2010

Descripción:

Esta actualización de seguridad resuelve una vulnerabilidad de la que se ha informado de forma pública en VBScript en Microsoft Windows que podría permitir la ejecución remota de código.

Productos Afectados:

Esta actualización de seguridad se considera importante para Microsoft Windows 2000, Windows XP y Windows Server 2003. En Windows Server 2008, Windows Vista, Windows 7 y Windows Server 2008 R2, no se puede aprovechar el código vulnerable; no obstante, como el código está presente, esta actualización se proporciona como medida defensiva y no tiene clasificación de gravedad.

Notas:

La actualización de seguridad corrige la vulnerabilidad al modificar la forma en que el motor de VBScript procesa los archivos de ayuda en modo protegido.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-022.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0483>

CVEs:

CVE-2010-0483

Sistemas Operativos - Una vulnerabilidad en Microsoft Office Publisher podría permitir la ejecución remota de código (981160)

Fecha: 4/13/2010

Descripción:

Esta actualización de seguridad resuelve una vulnerabilidad de la que se ha informado de forma privada en Microsoft Office Publisher que podría permitir la ejecución remota de código si un usuario abre un archivo de Publisher especialmente diseñado. Un intruso que aprovechara esta vulnerabilidad podría conseguir el mismo nivel de derechos de usuario que el usuario local. 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 importante para las versiones compatibles de Microsoft Office Publisher 2002, Microsoft Office Publisher 2003 y Microsoft Office Publisher 2007.

Notas:

La actualización corrige la vulnerabilidad al modificar la manera en que Microsoft Office Publisher abre los archivos de Publisher especialmente diseñados.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-023.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0479>

CVEs:

CVE-2010-0479

Sistemas Operativos - Vulnerabilidades en Microsoft Exchange y el servicio SMTP de Windows podrían permitir la denegación de servicio (981832)

Fecha: 4/13/2010

Descripción:

Esta actualización de seguridad resuelve una vulnerabilidad de la que se ha informado de forma pública y una vulnerabilidad de la que se ha informado de forma privada en Microsoft Exchange y en el servicio SMTP de Windows. La más grave de estas vulnerabilidades podría permitir la denegación de servicio si un atacante envía una respuesta DNS especialmente diseñada a un equipo que ejecuta el servicio SMTP. De forma predeterminada, el componente SMTP no está instalado en Windows Server 2003, Windows Server 2003 x64 Edition o Windows XP Professional x64 Edition.

Productos Afectados:

Esta actualización de seguridad se considera importante para todas las ediciones compatibles de Microsoft Windows 2000, Windows XP, Windows Server 2003, las ediciones de 32 bits y x64 de Windows Server 2008, Windows Server 2008 R2 para sistemas x64 y Microsoft Exchange Server 2003. Esta actualización de seguridad se considera moderada para Microsoft Exchange Server 2000.

Notas:

La actualización de seguridad corrige las vulnerabilidades al modificar la manera en que SMTP analiza los registros MX y el modo en que SMTP asigna memoria para interpretar las respuestas de comandos SMTP.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-024.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0024>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0025>

CVEs:

CVE-2010-0024, CVE-2010-0025

Sistemas Operativos - Una vulnerabilidad en Servicios de Microsoft Windows Media podría permitir la ejecución remota de código (980858)

Fecha: 4/13/2010

Descripción:

Esta actualización de seguridad resuelve una vulnerabilidad de la que se ha informado de forma privada en Servicios de Windows Media en Microsoft Windows 2000 Server. La vulnerabilidad podría permitir la ejecución remota de código si un atacante envía un paquete de información de transporte especialmente diseñado a un sistema Microsoft Windows 2000 Server que ejecute Servicios de Windows Media. Los procedimientos recomendados para firewall y las configuraciones de firewall predeterminadas estándar pueden proteger a las redes de los ataques procedentes del exterior del perímetro de la empresa. Se recomienda que los sistemas conectados a Internet tengan expuesta la cantidad mínima de puertos. En Microsoft Windows 2000 Server, Servicios de Windows Media es un componente opcional y no se instala de forma predeterminada.

Productos Afectados:

Esta actualización de seguridad se considera crítica para todas las ediciones compatibles de Microsoft Windows 2000 Server.

Notas:

La actualización de seguridad corrige la vulnerabilidad al modificar la forma en que el servicio de unidifusión de Windows Media (nsum.exe) trata los paquetes de red de información de transporte.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-025.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0478>

CVEs:

CVE-2010-0478

Sistemas Operativos - Una vulnerabilidad en los códecs MPEG Layer-3 de Microsoft podría permitir la ejecución remota de código (977816)

Fecha: 4/13/2010

Descripción:

Esta actualización de seguridad resuelve una vulnerabilidad de la que se ha informado de forma privada en los códecs de audio MPEG Layer-3 de Microsoft. La vulnerabilidad podría permitir la ejecución remota de código si un usuario abre un archivo AVI especialmente diseñado que contenga una secuencia de audio MPEG Layer-3. Si un usuario inicia sesión con derechos de usuario administrativos, un intruso que aprovechara esta vulnerabilidad podría lograr el control completo de un sistema afectado. De esta forma, un intruso podría instalar programas; ver, cambiar o eliminar datos; o crear cuentas nuevas con todos los derechos de usuario. 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 ediciones compatibles de Microsoft Windows 2000, Windows XP, Windows Server 2003 (excepto las ediciones para sistemas con Itanium) y Windows Server 2008 (excepto las ediciones para sistemas con Itanium). Para todas las ediciones compatibles de Windows Vista, esta actualización de seguridad se considera importante. Las ediciones para sistemas con Itanium de Windows Server 2003 y Windows Server 2008, y todas las ediciones compatibles de Windows 7 y Windows Server 2008 R2 no están afectadas por la vulnerabilidad.

Notas:

La actualización de seguridad corrige la vulnerabilidad al modificar la forma en que los códecs de audio MPEG Layer-3 de Microsoft descodifican la secuencia de audio MPEG Layer-3 en archivos AVI especialmente diseñados.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-026.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0480>

CVEs:

CVE-2010-0480

Sistemas Operativos - Una vulnerabilidad en el Reproductor de Windows Media podría permitir la ejecución remota de código (979402)

Fecha: 4/13/2010

Descripción:

Esta actualización de seguridad resuelve una vulnerabilidad en Reproductor de Windows Media de la que se ha informado de forma privada. La vulnerabilidad podría permitir la ejecución remota de código si Reproductor de Windows Media abre contenido multimedia especialmente diseñado hospedado en un sitio web malintencionado. Un intruso que aprovechara esta vulnerabilidad podría conseguir el mismo nivel de derechos de usuario que el usuario local. 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 Reproductor de Windows Media Serie 9 cuando está instalado en todas las ediciones compatibles de Microsoft Windows 2000 y Windows XP.

Notas:

La actualización de seguridad corrige la vulnerabilidad al modificar la forma en que el control ActiveX de Reproductor de Windows Media trata el contenido multimedia especialmente diseñado hospedado en un sitio web malintencionado.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-027.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0268>

CVEs:

CVE-2010-0268

Sistemas Operativos - Vulnerabilidades en Microsoft Visio podrían permitir la ejecución remota de código (980094)

Fecha: 4/13/2010

Descripción:

Esta actualización de seguridad resuelve dos vulnerabilidades de las que se ha informado de forma privada en Microsoft Office Visio. Las vulnerabilidades podrían permitir la ejecución remota de código si un usuario abre un archivo de Visio especialmente diseñado. Un intruso que aprovechara estas vulnerabilidades podría conseguir el mismo nivel de derechos de usuario que el usuario local. 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 importante para Microsoft Office Visio 2002 Service Pack 2, Microsoft Office Visio 2003 Service Pack 3, Microsoft Office Visio 2007 Service Pack 1 y Microsoft Office Visio 2007 Service Pack 2.

Notas:

La actualización de seguridad corrige estas vulnerabilidades al modificar la manera en que Microsoft Office Visio valida los atributos y calcula los índices al abrir archivos de Visio especialmente diseñados.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-028.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0254>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0256>

CVEs:

CVE-2010-0254, CVE-2010-0256

Sistemas Operativos - Una vulnerabilidad en el componente ISATAP de Windows podría permitir la suplantación de personalidad (978338)

Fecha: 4/13/2010

Descripción:

Esta actualización de seguridad crítica resuelve una vulnerabilidad de la que se ha informado de forma privada en Microsoft Windows. Esta actualización de seguridad se considera moderada para Windows XP, Windows Server 2003, Windows Vista y Windows Server 2008. Windows 7 y Windows Server 2008 R2 no son vulnerables porque estos sistemas operativos incluyen la característica implementada por esta actualización de seguridad.

Productos Afectados:

Esta actualización de seguridad se considera moderada para Windows XP, Windows Server 2003, Windows Vista y Windows Server 2008. Windows 7 y Windows Server 2008 R2 no son vulnerables porque estos sistemas operativos incluyen la característica implementada por esta actualización de seguridad.

Notas:

Esta vulnerabilidad podría permitir que un atacante suplantara una dirección IPv4 de modo que podría pasar por alto los dispositivos de filtrado que se basan en la dirección IPv4 de origen. La actualización de seguridad corrige la vulnerabilidad al cambiar la manera en que la pila TCP/IP de Windows comprueba la dirección IPv6 de origen en un paquete ISATAP de túnel.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-029.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0812>

CVEs:

CVE-2010-0812

Aplicaciones Usuario - Alerta de Seguridad en el producto Sun Java System Access Manager

Fecha: 4/12/2010

Descripción:

Esta alerta cubre el CVE-2010-0894 que afecta al producto Sun Java System Access Manager

Productos Afectados:

SPARC Platform

Sun Java System Access Manager 7 2005Q4 (for Solaris 8, 9 and 10) without patch 120954-11

Sun Java System Access Manager 7.1 (for Solaris 8, 9 and 10) without patch 126356-04

x86 Platform

Sun Java System Access Manager 7 2005Q4 (for Solaris 9 and 10) without patch 120955-11

Sun Java System Access Manager 7.1 (for Solaris 8, 9 and 10) without patch 126357-04

Linux Platform

Sun Java System Access Manager 7 2005Q4 without patch 120956-11

Sun Java System Access Manager 7.1 without patch 126358-04

Windows Platform

Sun Java System Access Manager 7 2005Q4 without patch 124296-11

Sun Java System Access Manager 7.1 without patch 126359-04

HP-UX

Sun Java System Access Manager 7 2005Q4 without patch 126371-11

Other

Sun Java System Access Manager 7.1 WAR file-based installation (all supported platforms) without patch 140504-04

OpenSSO Enterprise 8.0 (for all supported platforms) without patch 141655-03

Notas:

Solución:

Instalar los siguientes parches:

SPARC Platform

Sun Java System Access Manager 7 2005Q4 (for Solaris 8, 9 and 10) with patch 120954-11 or later

Sun Java System Access Manager 7.1 (for Solaris 8, 9 and 10) with patch 126356-04 or later
x86 Platform

Sun Java System Access Manager 7 2005Q4 (for Solaris 9 and 10) with patch 120955-11 or later
Sun Java System Access Manager 7.1 (for Solaris 8, 9 and 10) with patch 126357-04 or later
Linux Platform

Sun Java System Access Manager 7 2005Q4 with patch 120956-11 or later
Sun Java System Access Manager 7.1 with patch 126358-04 or later
Windows Platform

Sun Java System Access Manager 7 2005Q4 with patch 124296-11 or later
Sun Java System Access Manager 7.1 with patch 126359-04 or later
HP-UX

Sun Java System Access Manager 7 2005Q4 with patch 126371-11 or later
Other

OpenSSO Enterprise 8.0 (all supported platforms) with patch 141655-03 or later
Sun Java System Access Manager 7.1 WAR file-based installation (all supported platforms) with patch 140504-04 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-267568-1>

CVEs:

CVE-2010-0894

Sistemas Operativos - Alerta de seguridad en "kernel component" de Solaris y OpenSolaris

Fecha: 4/12/2010

Descripción:

Se ha descubierto un problema de seguridad en "kernel component" que afecta a los sistemas Solaris y OpenSolaris

Productos Afectados:

SPARC Platform

Solaris 10 without patch 138888-01

OpenSolaris based upon builds snv_01 through snv_98

x86 Platform

Solaris 10 without patch 138889-01

OpenSolaris based upon builds snv_01 through snv_98

Notas:

Solución:

Instalar los siguientes parches:

SPARC Platform

Solaris 10 with patch 138888-01 or later

OpenSolaris based upon builds snv_99 or later

x86 Platform

Solaris 10 with patch 138889-01 or later

OpenSolaris based upon builds snv_99 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-242386-1>

CVEs:

Aplicaciones Usuario - Vulnerabilidad en el Demonio NTP

Fecha: 4/12/2010

Descripción:

Se ha encontrado una vulnerabilidad en el demonio NTP (xntpd) que podría provocar un consumo excesivo de CPU, pudiendo provocar una denegación de servicio.

Productos Afectados:

SPARC Platform

Solaris 8

Solaris 9 without patch 117143-02

Solaris 10 xntpd (SUNWntpu) without patch 127724-02

Solaris 10 ntpd (SUNWntp4u) without patch 143725-01

OpenSolaris based upon builds snv_01 through snv_132

x86 Platform

Solaris 8

Solaris 9 without patch 117144-02

Solaris 10 xntpd (SUNWntpu) without patch 127725-02
Solaris 10 ntpd (SUNWntp4u) without patch 143726-01

OpenSolaris based upon builds snv_01 through snv_132

Notas:

Solución: Instalar las siguientes actualizaciones de seguridad:

SPARC Platform

Solaris 9 with patch 117143-02 or later

Solaris 10 xntpd (SUNWntpu) with patch 127724-02 or later

Solaris 10 ntpd (SUNWntp4u) with patch 143725-01 or later
OpenSolaris based upon builds snv_133
x86 Platform

Solaris 9 with patch 117144-02 or later

Solaris 10 xntpd (SUNWntpu) with patch 127725-02 or later
Solaris 10 ntpd (SUNWntp4u) with patch 143726-01 or later
OpenSolaris based upon builds snv_133

Referencias en la web:

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

CVEs:

Aplicaciones Usuario - Alerta de seguridad en el componente "Directory Server" de los productos Sun ONE Directory Server y Sun Java System Directory Server

Fecha: 4/12/2010

Descripción:

La vulnerabilidad que afecta a estos dos productos se describe en el CVE-2009-2404 y el CVE-2009-0688

Productos Afectados:

Sun Java System Directory Server 5.2:

Solaris 8, 9 and 10 on SPARC and x86 Platforms, Linux, Windows, HP-UX, and AIX:

Native Package Versions:

Sun ONE Directory Server 5.2

Sun Java System Directory Server 5 2003Q4 (5.2patch1)

Sun Java System Directory Server 5 2004Q2 (5.2patch2)

Sun Java System Directory Server 5 2005Q1 (5.2patch3)

Sun Java System Directory Server 5 2005Q4 (5.2patch4)

PatchZIP (Compressed Archive) Versions:

Sun ONE Directory Server 5.2

Sun Java System Directory Server 5.2 Patch2

Sun Java System Directory Server 5.2 Patch3

Sun Java System Directory Server 5.2 Patch4

Sun Java System Directory Server 5.2 Patch6 without patch 142806-01

Sun Java System Directory Server Enterprise Edition:

Solaris 9 and 10 on SPARC and x86 Platform, HP-UX, Linux, and Windows:

PatchZIP (Compressed Archive) and Native Package Versions:

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

Sun Java System Directory Server Enterprise Edition 6.3.1 without patch 142807-01 (for PatchZIP)

Notas:

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-273910-1>

CVEs:

CVE-2009-2404, CVE-2009-0688

Aplicaciones Usuario - Vulnerabilidad de seguridad en la utilidad "automake" de Solaris

Fecha: 4/15/2010

Descripción:

Se ha descubierto una vulnerabilidad que afecta a la herramienta "automake" de Solaris, pudiendo permitir que un usuario local sin privilegios pueda realizar cambios en los ficheros de paquetes, o ejecutar código arbitrario con los privilegios de otro usuario local que esté ejecutando "dist" y "distcheck".

Productos Afectados:

SPARC Platform

OpenSolaris based upon builds snv_71 through snv_131

x86 Platform

OpenSolaris based upon builds snv_71 through snv_131

Notas:

Solución: Instalar los siguientes parches:

SPARC Platform

OpenSolaris based upon builds snv_132 or later

x86 Platform

OpenSolaris based upon builds snv_132 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-275650-1>

CVEs:

Sistemas Operativos - Vulnerabilidades en el Kernel de SUSE

Fecha: 4/7/2010

Descripción:

Se han encontrado vulnerabilidades que afectan a los siguientes programas y módulos:

- gnome-screensaver
- tomcat5, tomcat6
- libtheora
- java-1_6_0-sun
- samba

Productos Afectados:

SLES9

SLE10-SP2

SLE10-SP3

SLE11

openSUSE 11.0,11.1, 11.2

Notas:

Más información en:

http://www.novell.com/linux/security/advisories/2010_8_sr.html

Referencias en la web:

http://www.novell.com/linux/security/advisories/2010_8_sr.html

CVEs:

CVE-2008-5515, CVE-2009-2693, CVE-2009-2901, CVE-2009-2902, CVE-2009-3389, CVE-2009-3555, CVE-2010-0082, CVE-2010-0084, CVE-2010-0085, CVE-2010-0087, CVE-2010-0088, CVE-2010-0089, CVE-2010-0090, CVE-2010-0091, CVE-2010-0092, CVE-2010-0093, CVE-2010-0094, CVE-2010-0095, CVE-2010-0547, CVE-2010-0732, CVE-2010-0837, CVE-2010-0838, CVE-2010-0839, CVE-2010-0840, CVE-2010-0841, CVE-2010-0842, CVE-2010-0843, CVE-2010-0844, CVE-2010-0845, CVE-2010-0846, CVE-2010-0847, CVE-2010-0848, CVE-2010-0849, CVE-2010-0850, CVE-2010-0926

Sistemas Operativos - Vulnerabilidades en el Kernel de SUSE

Fecha: 4/14/2010

Descripción:

Se han publicado diversas vulnerabilidades que afectan a los siguientes módulos y aplicaciones:

- viewvc
- krb5
- pango
- gimp
- kdatabase3, kde4-kdm

Productos Afectados:

SLE10-SP2, SLE10-SP3, SLE11, openSUSE 11.0, 11.1, 11.2

Notas:

Más información en: http://www.novell.com/linux/security/advisories/2010_9_sr.html

Referencias en la web:

http://www.novell.com/linux/security/advisories/2010_9_sr.html

CVEs:

CVE-2009-1570, CVE-2009-3909, CVE-2010-0132, CVE-2010-0421, CVE-2010-0436, CVE-2010-0629

Sistemas Operativos - Bug fix en el Kernel de Red Hat Linux

Fecha: 4/6/2010

Descripción:

Se ha publicado la solución a un problema de seguridad en el Kernel de Red Hat. Este problema afecta a la función `sctp_rcv_ootb()` del protocolo de control de Transmisión de flujo de datos (Stream) del kernel.

Además, este parche soluciona el problema relacionado con la funcionalidad Wake on LAN en los drivers Intel PRO/1000 Linux, y e1000e.

Productos Afectados:

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

Notas:

Se puede encontrar más información en:

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

Referencias en la web:

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

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-275650-1>

CVEs:

CVE-2010-0008

Aplicaciones Usuario - Actualización de krb5

Fecha: 4/6/2010

Descripción:

Se han actualizado los paquetes de krb5, solucionando problemas en el demonio MIT Kerberos (kadmind). Las vulnerabilidades que afectaban al demonio eran explotables sin necesidad de privilegios.

También se han solucionado problemas relacionadas con el KDC (Key Distribution Center).

Productos Afectados:

RHEL Desktop Workstation (v. 5 client) - i386, x86_64 Red Hat Enterprise Linux (v. 5 server) - i386, ia64, ppc, s390x, x86_64 Red Hat Enterprise Linux Desktop (v. 5 client) - i386, x86_64

Notas:

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

Referencias en la web:

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

CVEs:

CVE-2010-0629

Bases de Datos - Nevos paquetes nss_db que solucionan varios problemas de seguridad

Fecha: 4/13/2010

Descripción:

Se han publicado nuevos paquetes de nss_db para Red Hat Linux 5 que solucionan el problema de que nss_db no especifique un path al directorio que se va a usar para el entorno de Base de Datos de la librería de Base de Datos Berkeley, causando que el directorio a utilizar sea el por defecto, y permitiendo a los usuarios locales poder obtener información sensible.

Productos Afectados:

Red Hat Enterprise Linux (v. 5 server) - i386, ia64, ppc, s390x, x86_64 Red Hat Enterprise Linux Desktop (v. 5 client) - i386, x86_64

Notas:

Se puede obtener más información en:

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

Referencias en la web:

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

CVEs:

CVE-2010-0826

Sistemas Operativos - Actualización importante en kdebase

Fecha: 4/14/2010

Descripción:

Se han actualizado los paquetes de kdebase para Red Hat Linux 4 y 5 para solventar la siguiente vulnerabilidad:

Se encontró una vulnerabilidad que permitía la escalada de privilegios en el KDE Display Manager. Un usuario local con acceso a la consola podría provocar una condición "race", resultando en la obtención de privilegios de escritura sobre un fichero aleatorio.

Productos Afectados:

RHEL Desktop Workstation (v. 5 client) - i386, x86_64 Red Hat Enterprise Linux (v. 5 server) - i386, ia64, ppc, s390x, x86_64 Red Hat Enterprise Linux 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 4 - i386, ia64, x86_64 Red Hat Enterprise Linux WS version 4 - i386, ia64, x86_64

Notas:

Más información:

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

Referencias en la web:

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

CVEs:

CVE-2010-0436

Aplicaciones Usuario - Actualización de seguridad en Acroread

Fecha: 4/14/2010

Descripción:

Esta actualización de seguridad soluciona varios problemas de seguridad en Adobe Reader.

Todas ellas son explotables mediante un fichero pdf especialmente diseñado que puede permitir la ejecución de código arbitrario.

Productos Afectados:

RHEL Desktop Supplementary (v. 5 client) - i386, x86_64 RHEL Supplementary (v. 5 server) - i386, x86_64 Red Hat Desktop version 4 Extras - i386, x86_64 Red Hat Enterprise Linux AS version 4 Extras - i386, 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:

Más información en:

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

Referencias en la web:

<https://rhn.redhat.com/errata/RHSA-2010-0349.html>

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

CVEs:

CVE-2010-0190 CVE-2010-0191 CVE-2010-0192 CVE-2010-0193 CVE-2010-0194 CVE-2010-0195 CVE-2010-0196 CVE-2010-0197 CVE-2010-0198 CVE-2010-0199 CVE-2010-0201 CVE-2010-0202 CVE-2010-0203 CVE-2010-0204 CVE-2010-1241

Bases de Datos - Oracle Critical Patch Update Advisory - April 2010

Fecha: 4/1/2010

Descripción:

La actualización contiene 47 nuevos parches de seguridad para diversos productos

Productos Afectados:

- Oracle Database 11g Release 2, version 11.2.0.1 [Database]
- Oracle Database 11g Release 1, version 11.1.0.7 [Database]
- Oracle Database 10g Release 2, versions 10.2.0.3, 10.2.0.4 [Database]
- Oracle Database 10g, version 10.1.0.5 [Database]
- Oracle Database 9i Release 2, versions 9.2.0.8, 9.2.0.8DV [Database]
- Oracle Application Server 10gR2, version 10.1.2.3.0 [Fusion Middleware]
- Oracle Identity Management 10g, version 10.1.4.0.1 and 10.1.4.3 [Fusion Middleware]
- Oracle Collaboration Suite 10g, version 10.1.2.4 [Collaboration Suite]
- Oracle E-Business Suite Release 12, versions 12.0.4, 12.0.5, 12.0.6, 12.1.1 and 12.1.2 [E-Business Suite]
- Oracle E-Business Suite Release 11i, versions 11.5.10, 11.5.10.2 [E-Business Suite]
- Oracle Transportation Manager, Versions: 5.5.05.07, 5.5.06.00, 6.0.03 [Oracle Transportation Management]
- Oracle Agile - Engineering Data Management, Version 6.1.1.0 [Agile - Engineering Data Management]
- PeopleSoft Enterprise PeopleTools, versions 8.49 and 8.50 [PeopleSoft/JDE]
- Oracle Communications Unified Inventory Management version 7.1 [Communications Industry Suite]
- Oracle Clinical Remote Data Capture Option 4.5.3, 4.6 [Life Sciences Industry Suite]
- Oracle Thesaurus Management System 4.5.2, 4.6, 4.6.1 [Life Sciences Industry Suite]
- Oracle Retail Markdown Optimization version 13.1 [Retail Industry Suite]
- Oracle Retail Place In-Season version 12.2 [Retail Industry Suite]
- Oracle Retail Plan In-Season version 12.2 [Retail Industry Suite]
- Oracle Sun Product Suite [Oracle Sun Product Suite]

Notas:

Referencias en la web:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2010.html>

CVEs:

CVE-2010-0853 CVE-2010-0860 CVE-2010-0866 CVE-2010-0852 CVE-2010-0867 CVE-2010-0851 CVE-2010-0870 CVE-2010-0854

Aplicaciones Usuario - Security Notice for CA Xosoft

Fecha: 4/6/2010

Descripción:

El soporte de CA alerta de diversos riesgos de seguridad sobre CA XOssoft. Existe multiples vulnerabilidades que pueden permitir a un atacante externo obtener información sensible, causar denegación de servicio o ejecutar código arbitrario. CA ya ha publicado parchas para solucionar dichos problemas.

Productos Afectados:

CA XOssoft Replication r12.5

CA XOssoft High Availability r12.5

CA XOssoft Content Distribution r12.5

CA XOssoft Replication r12.0

CA XOssoft High Availability r12.0

CA XOssoft Content Distribution r12.0

Notas:

Productos no afectados:

CA XOssoft Replication r4

CA XOssoft High Availability r4

CA XOssoft Content Distribution r4

Referencias en la web:

<https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=232869>

CVEs:

CVE-2010-1221 CVE-2010-1222 CVE-2010-1223

Sistemas Operativos - VMware Security Advisory

Fecha: 4/9/2010

Descripción:

Los productos de VMware basados en host, vCenter Server y ESX contienen diversas vulnerabilidades de seguridad:

- Windows-based VMware Tools Unsafe Library Loading vulnerability
- Windows-based VMware Tools Arbitrary Code Execution vulnerability
- Windows-based VMware Workstation and Player host privilege escalation
- Third party library update for libpng to version 1.2.37
- VMware VMnc Codec heap overflow vulnerabilities
- VMware Remote Console format string vulnerability
- Windows-based VMware authd remote denial of service
- Potential information leak via hosted networking stack
- Linux-based vmrun format string vulnerability

Productos Afectados:

VMware Workstation 7.0, VMware Workstation 6.5.3 and earlier, VMware Player 3.0, VMware Player 2.5.3 and earlier, VMware ACE 2.6, VMware ACE 2.5.3 and earlier, VMware Server 2.0.2 and earlier, VMware Fusion 3.0, VMware Fusion 2.0.6 and earlier, VMware VIX API for Windows 1.6.x, VMware ESXi 4.0 before patch ESXi400-201002402-BG, VMware ESXi 3.5 before patch ESXe350-200912401-T-BG, VMware ESX 4.0 without patches ESX400-201002401-BG, ESX400-200911223-UG, VMware ESX 3.5 without patch ESX350-200912401-BG, VMware ESX 3.0.3 without patch ESX303-201002203-UG, VMware ESX 2.5.5 without Upgrade Patch 15.

Notas:

Referencias en la web:

<http://www.vmware.com/security/advisories/VMSA-2010-0007.html>

CVEs:

CVE-2010-1141

