

BOLETÍN DE VULNERABILIDADES
ÁUDEA, SEGURIDAD DE LA INFORMACIÓN
15 DE FEBERRO 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 - MS10-003 – Crítico - 2/9/2010 - Una vulnerabilidad en Microsoft Office (MSO) podría permitir la ejecución remota de código (978214)**
- **Aplicaciones Usuario - MS10-004 – Importante - 2/9/2010 - Vulnerabilidades en Microsoft Office PowerPoint podrían permitir la ejecución remota de código (975416)**
- **Aplicaciones Usuario - MS10-005 – Moderado - 2/9/2010 - Una vulnerabilidad en Microsoft Paint podría permitir la ejecución remota de código (978706)**
- **Sistemas Operativos - MS10-006 – Crítico - 2/9/2010 - Vulnerabilidades en el cliente SMB podrían permitir la ejecución remota de código (978251)**
- **Sistemas Operativos - MS10-007 – Crítico - 2/9/2010 - Una vulnerabilidad en el controlador del shell de Windows podría permitir la ejecución remota de código (975713)**
- **Sistemas Operativos - MS10-008 – Crítico - 2/9/2010 - Actualización de seguridad acumulativa de bits de interrupción de ActiveX (978262)**
- **Sistemas Operativos - MS10-009 – Crítico - 2/9/2010 - Vulnerabilidades en TCP/IP de Windows podrían permitir la ejecución remota de código (974145)**
- **Sistemas Operativos - MS10-010 - Importante - 2/9/2010 - Una vulnerabilidad en Windows Server 2008 Hyper-V podría permitir la denegación de servicio (977894)**
- **Sistemas Operativos - MS10-011 - Importante - 2/9/2010 - Una vulnerabilidad en el subsistema de tiempo de ejecución de cliente-servidor de Windows podría permitir la elevación de privilegios (978037).**
- **Sistemas Operativos - MS10-012 - Importante - 2/9/2010 - Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código (971468)**
- **Sistemas Operativos - MS10-013 – Crítico - 2/9/2010 - Una vulnerabilidad en Microsoft DirectShow podría permitir la ejecución remota de código (977935)**
- **Sistemas Operativos - MS10-014 - Importante - 2/9/2010 - Una vulnerabilidad en Kerberos podría permitir la denegación de servicio (977290)**
- **Sistemas Operativos - MS10-015 - Importante - 2/9/2010 - Vulnerabilidades del kernel de Windows podrían permitir la elevación de privilegios (977165)**
- **Aplicaciones Usuario - 6908614 /Sun Microsystems - 2/1/2010 - Varias vulnerabilidades en Adobe Flash Player para Solaris**
- **Sistemas Operativos - 6907934 /Sun Microsystems - 2/1/2010 - Algunos parches para Sun Cluster 3.2 Quorum Server causan una situación de "pánico" en todos los nodos del kernel, con el siguiente error: "Cluster lost operational quorum".**
- **Sistemas Operativos - 6912597 /Sun Microsystems - 2/3/2010 - Interfaz Gráfica de Sun Blade X6270 inaccesible en los Blades recién instalados**

- **Sistemas Operativos - 6913788, 6913833 /Sun Microsystems - 2/3/2010 - Vulnerabilidad de seguridad existente tras unir un Sistema OpenSolaris a un Dominio Windows utilizando kclient(1M) o smadm(1M)**
- **Servicios (ftp, www, dns, etc.) - 6916389 /Sun Microsystems - 2/4/2010 - Varias vulnerabilidades en los métodos de autenticación HTTP TRACE, WebDav, y Digest de Servidor Sun Java System Web Server y el Servidor Sun Java System Web Proxy Server**
- **Aplicaciones Usuario - 6588160 /Sun Microsystems - 2/4/2010 - Vulnerabilidad en Java Runtime Environment con los usuarios autenticados mediante kerberos**
- **Sistemas Operativos - 6915592 /Sun Microsystems - 2/4/2010 – Problema Driver Patch SPARC 141874-06 para Solaris 10 Fibre Channel fp (7d)**
- **Servicios (ftp, www, dns, etc.) - 6902029 /Sun Microsystems - 2/8/2010 - Vulnerabilidad de seguridad en el demonio NTP(xntpd(1M))**
- **Sistemas Operativos - 6902220, 6877035 /Sun Microsystems - 2/8/2010 - Error de arranque del sistema al realizar la actualización de Zpool.**
- **Sistemas Operativos - 6890136 /Sun Microsystems - 2/10/2010 - Error en los parches OBP para los firmwares 4.30.3, 4.30.3b, o 4.30.4 (WITHDRAWN)**
- **Servicios (ftp, www, dns, etc.) - 6899619, 6898371 /Sun Microsystems - 2/10/2010 - Vulnerabilidades de seguridad en la Transport Layer Security (TLS) y Secure Sockets Layer 3.0 (SSLv3)**
- **Sistemas Operativos - SUSE-SR:2010:002 - 2/1/2010 - Resumen de Seguridad de SUSE:**
- **Sistemas Operativos - SUSE-SA:2010:009 - 2/5/2010 - Vulnerabilidad de Denegación de Servicio en Linux Kernel**
- **Sistemas Operativos - HT4013 - 2/2/2010 - Contenido de seguridad de iPhone OS 3.1.3 y iPhone OS 3.1.3 para iPod touch**

2. Boletín Detallado Vulnerabilidades

Aplicaciones Usuario - Una vulnerabilidad en Microsoft Office (MSO) podría permitir la ejecución remota de código (978214)

Fecha: 2/9/2010

Descripción:

Esta actualización de seguridad resuelve una vulnerabilidad de la que se ha informado de forma privada en Microsoft Office que podría permitir la ejecución remota de código si un usuario abre un archivo de Office especialmente diseñado. Un atacante 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 importante para todas las ediciones compatibles de Microsoft Office XP y Microsoft Office 2004 para Mac.

Notas:

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

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-003.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0243>

CVEs:

CVE-2010-0243

Aplicaciones Usuario - Vulnerabilidades en Microsoft Office PowerPoint podrían permitir la ejecución remota de código (975416)

Fecha: 2/9/2010

Descripción:

Esta actualización de seguridad resuelve seis vulnerabilidades de las que se ha informado de forma privada en Microsoft Office PowerPoint. Las vulnerabilidades podrían permitir la ejecución remota de código si un usuario abre un archivo de PowerPoint especialmente diseñado. 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 importante para las ediciones compatibles de Microsoft Office PowerPoint 2002, Microsoft Office PowerPoint 2003 y Microsoft Office 2004 para Mac.

Notas:

La actualización de seguridad corrige las vulnerabilidades al modificar la forma en que Microsoft Office PowerPoint y Microsoft PowerPoint Viewer analizan los archivos de PowerPoint especialmente diseñados.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-004.msp>

<http://cve.mitre.org>

CVEs:

CVE-2010-0029, CVE-2010-0030, CVE-2010-0031, CVE-2010-0032, CVE-2010-0033, CVE-2010-0034

Aplicaciones Usuario - Una vulnerabilidad en Microsoft Paint podría permitir la ejecución remota de código (978706)

Fecha: 2/9/2010

Descripción:

Esta actualización de seguridad resuelve una vulnerabilidad de la que se ha informado de forma privada en Microsoft Paint. La vulnerabilidad podría permitir la ejecución remota de código si un usuario visualiza un archivo de imagen JPEG especialmente diseñado mediante Microsoft Paint. 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 moderada para Microsoft Windows 2000, Windows XP y Windows Server 2003.

Notas:

La actualización de seguridad corrige la vulnerabilidad al modificar la manera en que Microsoft Paint descodifica los archivos de imagen JPEG.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-005.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0028>

CVEs:

CVE-2010-0028

Sistemas Operativos - Vulnerabilidades en el cliente SMB podrían permitir la ejecución remota de código (978251)

Fecha: 2/9/2010

Descripción:

Esta actualización de seguridad resuelve dos 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 malintencionado.

Productos Afectados:

Esta actualización de seguridad se considera crítica para Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows 7 y Windows Server 2008 R2, e importante para todas las ediciones compatibles de Windows Vista y Windows Server 2008.

Notas:

La actualización de seguridad corrige las vulnerabilidades al modificar la manera en que el cliente SMB valida las respuestas.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-006.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0016>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0017>

CVEs:

CVE-2010-0016, CVE-2010-0017

Sistemas Operativos - Una vulnerabilidad en el controlador del shell de Windows podría permitir la ejecución remota de código (975713)

Fecha: 2/9/2010

Descripción:

Esta actualización de seguridad resuelve una vulnerabilidad de la que se ha informado de forma privada en Microsoft Windows 2000, Windows XP y Windows Server 2003. Otras versiones de Windows no están afectadas por esta actualización de seguridad. La vulnerabilidad podría permitir la ejecución remota de código si una aplicación, como un explorador web, pasa datos especialmente diseñados a la función de la API ShellExecute a través del controlador del shell de Windows.

Productos Afectados:

Esta actualización de seguridad se considera crítica para todas las ediciones compatibles de Microsoft Windows 2000, Windows XP y Windows Server 2003.

Notas:

La actualización de seguridad corrige la vulnerabilidad al modificar la forma en que la API ShellExecute valida los parámetros de entrada.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-007.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0027>

CVEs:

CVE-2010-0027

Sistemas Operativos - Actualización de seguridad acumulativa de bits de interrupción de ActiveX (978262)

Fecha: 2/9/2010

Descripción:

Esta actualización de seguridad corrige una vulnerabilidad de la que se ha informado de forma privada para el software de Microsoft. La vulnerabilidad podría permitir la ejecución remota de código si un usuario visita una página web especialmente diseñada que ejecuta un control ActiveX con Internet Explorer. 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. Esta actualización también incluye bits de interrupción para cuatro controles ActiveX de terceros.

Productos Afectados:

Esta actualización de seguridad se considera crítica para todas las ediciones compatibles de Microsoft Windows 2000 y Windows XP, importante para todas las ediciones compatibles de Windows Vista y Windows 7, moderada para todas las ediciones compatibles de Windows Server 2003 y baja para todas las ediciones compatibles de Windows Server 2008 y Windows Server 2008 R2.

Notas:

La actualización de seguridad corrige la vulnerabilidad al establecer un bit de interrupción para que el control vulnerable no se ejecute en Internet Explorer.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-008.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0252>

CVEs:

CVE-2010-0252

Sistemas Operativos - Vulnerabilidades en TCP/IP de Windows podrían permitir la ejecución remota de código (974145)

Fecha: 2/9/2010

Descripción:

Esta actualización de seguridad resuelve cuatro vulnerabilidades de las que se ha informado de forma privada en Microsoft Windows. La más grave de estas vulnerabilidades podría permitir la ejecución remota de código si se envían paquetes especialmente diseñados a un equipo con IPv6 habilitado. Un atacante podría intentar aprovechar la vulnerabilidad mediante la creación de paquetes ICMPv6 especialmente diseñados y su envío a un sistema como IPv6 habilitado. Esta vulnerabilidad sólo se puede aprovechar si el atacante está en el vínculo.

Productos Afectados:

Es una actualización de seguridad crítica para Windows Vista y Windows Server 2008.

Notas:

La actualización de seguridad corrige las vulnerabilidades al cambiar la forma en que Windows TCP/IP realiza las comprobaciones de límites y otras operaciones de tratamiento de paquetes.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-009.msp>

<http://cve.mitre.org>

CVEs:

CVE-2010-0239, CVE-2010-0240, CVE-2010-0241, CVE-2010-0242

Sistemas Operativos - Una vulnerabilidad en Windows Server 2008 Hyper-V podría permitir la denegación de servicio (977894)

Fecha: 2/9/2010

Descripción:

Esta actualización de seguridad resuelve una vulnerabilidad de la que se ha informado de forma privada en Windows Server 2008 Hyper-V y en Windows Server 2008 R2 Hyper-V. La vulnerabilidad podría permitir la denegación de servicio si un usuario ejecuta una secuencia con formato incorrecto de instrucciones máquina en una de las máquinas virtuales invitadas que hospede el servidor Hyper-V. Para aprovechar esta vulnerabilidad, el atacante debe tener credenciales de inicio de sesión válidas y ser capaz de iniciar una sesión localmente en una máquina virtual invitada. Los usuarios anónimos o los usuarios remotos no pueden aprovechar esta vulnerabilidad.

Productos Afectados:

Es una actualización de seguridad importante para todas las ediciones x64 compatibles de Microsoft Windows Server 2008 y Windows Server 2008 R2.

Notas:

La actualización de seguridad corrige la vulnerabilidad al modificar la manera en que el servidor Hyper-V valida la codificación en las instrucciones máquina ejecutadas en sus máquinas virtuales invitadas.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-010.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0026>

CVEs:

CVE-2010-0026

Sistemas Operativos - Una vulnerabilidad en el subsistema de tiempo de ejecución de cliente-servidor de Windows podría permitir la elevación de privilegios (978037).

Fecha: 2/9/2010

Descripción:

Esta actualización de seguridad resuelve una vulnerabilidad de la que se ha informado de forma privada en el subsistema de tiempo de ejecución de cliente-servidor de Microsoft Windows (CSRSS) en Microsoft Windows 2000, Windows XP y Windows Server 2003. Otras versiones de Windows no están afectadas. La vulnerabilidad podría permitir la elevación de privilegios si un atacante inicia sesión en el sistema y ejecuta una aplicación especialmente diseñada para seguir ejecutándose después de que el atacante cierre la sesión. Para aprovechar esta vulnerabilidad, un atacante debe de tener unas credenciales de inicio de sesión válidas y ser capaz de iniciar una sesión local. Usuarios remotos no pueden aprovechar esta vulnerabilidad.

Productos Afectados:

Esta actualización de seguridad se considera importante para todas las ediciones compatibles de Microsoft Windows 2000, Windows XP y Windows Server 2003.

Notas:

La actualización de seguridad corrige la vulnerabilidad al modificar la forma en que se finalizan los procesos de los usuarios al cerrar la sesión.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-011.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0023>

CVEs:

CVE-2010-0023

Sistemas Operativos - Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código (971468)

Fecha: 2/9/2010

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 ejecución remota de código si un atacante crea un paquete SMB especialmente diseñado y lo envía a un sistema afectado. 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 que intentan aprovechar estas vulnerabilidades.

Productos Afectados:

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

Notas:

La actualización de seguridad corrige estas vulnerabilidades al modificar la forma en que SMB valida las solicitudes SMB.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-012.msp>

<http://cve.mitre.org>

CVEs:

CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, CVE-2010-0031

Sistemas Operativos - Una vulnerabilidad en Microsoft DirectShow podría permitir la ejecución remota de código (977935)

Fecha: 2/9/2010

Descripción:

Esta actualización de seguridad crítica resuelve una vulnerabilidad de la que se ha informado de forma privada en Microsoft DirectShow. La vulnerabilidad podría permitir la ejecución remota de código si un usuario abre un archivo AVI especialmente diseñado. Un atacante 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, excepto para todas las ediciones con Itanium compatibles de Windows Server 2003, Windows Server 2008 y Windows Server 2008 R2, para las que esta actualización de seguridad se considera importante.

Notas:

La actualización de seguridad corrige la vulnerabilidad al modificar la forma en que DirectShow abre los archivos AVI.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-013.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0250>

CVEs:

CVE-2010-0250

Sistemas Operativos - Una vulnerabilidad en Kerberos podría permitir la denegación de servicio (977290)

Fecha: 2/9/2010

Descripción:

Esta actualización de seguridad crítica resuelve una vulnerabilidad de la que se ha informado de forma privada en Microsoft Windows. La vulnerabilidad podría permitir la denegación de servicio si se envía una solicitud de renovación de vale especialmente diseñada al dominio Windows Kerberos desde un usuario autenticado en un territorio de confianza que no es de Windows Kerberos. La denegación de servicio podría persistir hasta que se reinicie el controlador de dominio.

Productos Afectados:

Esta actualización de seguridad se considera importante para todas las ediciones compatibles de Microsoft Windows 2000 Server, Windows Server 2003 y Windows Server 2008.

Notas:

Esta actualización corrige la vulnerabilidad al modificar la forma en que el servidor Kerberos trata las solicitudes de renovación de vale.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-014.msp>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0035>

CVEs:

CVE-2010-0035

Sistemas Operativos - Vulnerabilidades del kernel de Windows podrían permitir la elevación de privilegios (977165)

Fecha: 2/9/2010

Descripción:

Esta actualización de seguridad resuelve una vulnerabilidad de la que se ha informado de forma pública y otra vulnerabilidad de las que se ha informado de forma privada en Microsoft Windows. Las vulnerabilidades podrían permitir la elevación de privilegios si un atacante ha iniciado sesión en el sistema y ha ejecutado una aplicación especialmente diseñada. Para aprovechar cualquiera de las vulnerabilidades, el atacante debe tener credenciales de inicio de sesión válidas y poder iniciar sesión. 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, Windows Vista, Windows Server 2008 y Windows 7 para sistemas de 32 bits.

Notas:

La actualización de seguridad corrige las vulnerabilidades al garantizar que el kernel de Windows trata las excepciones correctamente.

Referencias en la web:

<http://www.microsoft.com/spain/technet/security/bulletin/ms10-015.mspx>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0232>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0233>

CVEs:

CVE-2010-0232, CVE-2010-0233

Aplicaciones Usuario - Varias vulnerabilidades en Adobe Flash Player para Solaris

Fecha: 2/1/2010

Descripción:

Se han encontrado varias vulnerabilidades en Adobe Flash Player para Solaris (versiones 10.0.32.18), pudiendo permitir que un atacante provoque una Denegación de Servicio o una ejecución remota de código.

Productos Afectados:

SPARC Platform

Solaris 10 sin el parche 125332-08

OpenSolaris versiones desde la snv_01 a la snv_130

x86 Platform

Solaris 10 sin el parche 125333-08

OpenSolaris desde la versión snv_01 a la snv_130

Notas:

Instalar los siguientes parches de seguridad:

Solaris 10 con el parche 125332-08 o posterior.

OpenSolaris actualizado a la versión snv_131 o superior.

x86 Platform

Solaris 10 con el parche 125333-08 o superior

OpenSolaris actualizado a la versión snv_131 o superior

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-274250-1>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3794>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3796>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3797>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3798>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3799>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3800>

CVEs:

CVE-2009-3794, CVE-2009-3796, CVE-2009-3797, CVE-2009-3798, CVE-2009-3799, CVE-2009-3800

Sistemas Operativos - Algunos parches para Sun Cluster 3.2 Quorum Server causan una situación de "pánico" en todos los nodos del kernel, con el siguiente error: "Cluster lost operational quorum".

Fecha: 2/1/2010

Descripción:

Al instalar los parches de Sun Cluster 3.2 Quorum en el Servidor Quorum, provoca que todos los nodos de todos los clusters administrados por ese servidor provoquen el error: "Cluster lost operationel Quorum".

Productos Afectados:

SPARC Platform

Sun Cluster 3.2 (for Solaris 9) with patch 127404-03 or later

Sun Cluster 3.2 (for Solaris 10) with patch 127405-04 or later

x86 Platform

Sun Cluster 3.2 (for Solaris 10) with patch 127406-04 or later

Notas:

Solución:

Instalar los parches siguiendo las instrucciones indicadas en:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-275310-1>

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-275310-1>

CVEs:

Sistemas Operativos - Interfaz Gráfica de Sun Blade X6270 inaccesible en los Blades recién instalados

Fecha: 2/3/2010

Descripción:

Un fallo en la versión 2.1 (firmware 3.0.6.10) del Sun Blade X6270 provoca que el Interfaz Gráfica de Usuario Lights Out Manager (ILOM) estar inaccesible para los Blades recién instalados.

Productos Afectados:

Sun Blade X6270 Server Module

Notas:

Solución:

Actualizar el software a la siguiente versión:

x64 Platform

Sun Blade X6270 with ILOM firmware version 3.0.6.21 (Software 2.1.1) or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-276570-1>

CVEs:

Sistemas Operativos - Vulnerabilidad de seguridad existente tras unir un Sistema OpenSolaris a un Dominio Windows utilizando kclient(1M) o smadm(1M)

Fecha: 2/3/2010

Descripción:

Existe una vulnerabilidad en la configuración por defecto del cliente Kerberos (kclient(1M)), y en la utilidad de configuración CIFS (smbadm(1M)) cuando se une el sistema a un dominio Windows (Active Directory).

Productos Afectados:

SPARC Platform

OpenSolaris based upon builds snv_77 through snv_131 for smbadm(1M)

OpenSolaris based upon builds snv_91 through snv_131 for kclient(1M)

x86 Platform

OpenSolaris based upon builds snv_77 through snv_131 for smbadm(1M)

OpenSolaris based upon builds snv_91 through snv_131 for kclient(1M)

Notas:

Solución:

Instalar las siguientes actualizaciones:

SPARC Platform

OpenSolaris based upon builds snv_132 or later for smbadm(1M) and kclient(1M)

x86 Platform

OpenSolaris based upon builds snv_132 or later for smbadm(1M) and kclient(1M)

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-275790-1>

CVEs:

Servicios (ftp, www, dns, etc.) - Varias vulnerabilidades en los métodos de autenticación HTTP TRACE, WebDav, y Digest de Servidor Sun Java System Web Server y el Servidor Sun Java System Web Proxy Server

Fecha: 2/4/2010

Descripción:

Se han encontrado las siguientes vulnerabilidades en Sun Java System Web Server y Sun Java System Web Proxy Server:

-(BugIDs 6916389 and 6916390) Buffer overflow y vulnerabilidades en el formato de las cadenas de las extensiones de Webdav del Sun Java System Web Server. Estos problemas podrían permitir a los clientes provocar un bloqueo del servidor web, como resultado de una condición de Denegación de Servicio. Estos fallos también podrían permitir a usuarios remotos no autenticados realizar una elevación de privilegios, consiguiendo acceso de lectura/escritura a ficheros con información importante.

-(BugIDs 6916391 and 6917212) Problemas de Buffer overflow en los métodos de Autenticación Digest en el Sun Java System Web Server y Sun Java System Web Proxy Server, que podrían permitir a los usuarios remotos sin privilegios parar el servidor web o el servidor web proxy, provocando una situación de Denegación del Servicio. Estos problemas podrían permitir la ejecución de código arbitrario con un nivel alto de privilegios.

-(BugIDs 6916392 and 6917211) Problemas de Heap overflow en la funcionalidad HTTP TRACE del Sun Java System Web Server y el Sun Jav System Web Proxy Server, que podría permitir a usuarios remotos sin privilegios parar el servidor web y el el servidor web proxy, provocando una situación de Denegación de Servicio. Estos problemas podrían explotarse para obtener acceso no autorizado a información sensitiva.

Productos Afectados:

The issue described in BugID 6916389 can occur in the following releases for the SPARC, x86, Linux, Windows, HP-UX and AIX Platforms:

Sun Java System Web Server 7.0 without Update Release 8

The issues described in bugIDs 6916390, 6916391 and 6916392 can occur in the following releases for the SPARC, x86, Linux, Windows, HP-UX and AIX Platforms:

Sun Java System Web Server 7.0 without Update Release 8

Sun Java System Web Server 6.1 without Service Pack 12

The issues described in bugIDs 6917211 and 6917212 can occur in the following release for the SPARC, x86, Linux, Windows and HP-UX Platforms:

Sun Java System Web Proxy Server 4.0 without Service pack 13

Notas:

Solución: Instalar las siguientes actualizaciones:

Sun Java System Web Server 7.0 Release 8 or later

Sun Java System Web Server 6.1 Service Pack 12 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-275850-1>

CVEs:

Aplicaciones Usuario - Vulnerabilidad en Java Runtime Environment con los usuarios autenticados mediante kerberos

Fecha: 2/4/2010

Descripción:

Una vulnerabilidad de seguridad en el Java Runtime Environment afecta a los usuarios que se autentican mediante kerberos, pudiendo provocar una situación de Denegación de Servicio, así como un consumo excesivo de los recursos del sistema operativo.

Productos Afectados:

JDK and JRE 6 Update 10 or earlier

JDK and JRE 5.0 Update 16 or earlier

SDK and JRE 1.4.2_18 or earlier

Notas:

Solución:

Actualizar el software de Java a las siguientes versiones:

JDK and JRE 6 Update 11 or later

JDK and JRE 5.0 Update 17 or later

SDK and JRE 1.4.2_19 or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-246346-1>

CVEs:

Sistemas Operativos - ProblemaDriver Patch SPARC 141874-06 para Solaris 10 Fibre Channel fp (7d)

Fecha: 2/4/2010

Descripción:

El Driver Patch SPARC 141874-06 para Solaris 10 Fibre Channel fp (7d) puede provocar que los sistemas que utilizan el driver Fibre Channel fp(7d) alcance una situación "pánico".

Productos Afectados:

Solaris 10 with patch 141874-06 or later

Notas:

La solución a este problema aún no está disponible. Se espera que SUN la publica con la mayor brevedad posible.

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-276750-1>

CVEs:

Servicios (ftp, www, dns, etc.) - Vulnerabilidad de seguridad en el demonio NTP(xntpd(1M))

Fecha: 2/8/2010

Descripción:

Una vulnerabilidad de seguridad en el Demonio NTP (xntpd(1M)) asociado al NTP mode 7 (MODE_PRIVATE) puede provocar un consumo excesivo de CPU, resultando en una situación de Denegación de Servicio en el Servicio Solaris Network time Protocol.

Productos Afectados:

SPARC Platform

Solaris 8

Solaris 9

Solaris 10

OpenSolaris based upon builds snv_01 or later

x86 Platform

Solaris 8

Solaris 9

Solaris 10

OpenSolaris based upon builds snv_01 or later

Notas:

Solución:

Todavía no se ha publicado una solución para el problema.

Se prevee que SUN la publicará con la mayor brevedad posible.

Referencias en la web:

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

CVEs:

Sistemas Operativos - Error de arranque del sistema al realizar la actualización de Zpool.

Fecha: 2/8/2010

Descripción:

El parche del kernel 141445-09 para la plataforma Solaris 10 x86 ofrece soporte para una nueva versión de zpool. La nueva versión de zpool tiene dos problemas potenciales en sistemas con el sistema root ZFS, que provocan un fallo en el arranque.

Productos Afectados:

x86 Platform

Solaris 10 with patch 141445-09

Notas:

Solución:

Aún no se ha publicado una solución para el problema.

Se prevee que SUN publicará dicha solución con la mayor brevedad posible.

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-276010-1>

CVEs:

Sistemas Operativos - Error en los parches OBP para los firmwares 4.30.3, 4.30.3b, o 4.30.4 (WITHDRAWN)

Fecha: 2/10/2010

Descripción:

Los sistemas con los parches para los firmwares 4.30.3, 4.30.3b, o 4.30.4 (WITHDRAWN) fallan al arrancar si tienen una tarjeta PCI con un puente pci-pci instalado en ciertos slots PCI.

Productos Afectados:

SPARC Platform

Sun Fire V210/V240 Server with OBP firmware 4.30.3.b (as delivered in patch 142700-01)

Netra 210/240 Server with OBP firmware 4.30.3.b (as delivered in patch 142700-01)

Sun Blade 1500 Workstation (non Silver) with OBP firmware 4.30.3 (as delivered in patch 140686-01)

Sun Blade 2500 Workstation (non Silver) with OBP firmware 4.30.3 (as delivered in patch 140688-01)

Sun Blade 1500 Workstation Silver with OBP firmware 4.30.3 (as delivered in patch 140687-01)

Sun Blade 2500 Workstation Silver with OBP firmware 4.30.3 (as delivered in patch 140689-01)

Sun Fire V250 Server with OBP firmware 4.30.3 (as delivered in patch 140688-01)

Sun Fire V125 Server with OBP firmware 4.30.4 (as delivered in patch 142705-01)

Notas:

Solución: Instalar los siguientes parches:

SPARC Platform

Sun Fire V210/V240 Server with OBP firmware 4.30.4.a (as delivered in patch 142700-02) or later

Netra 210/240 Server with OBP firmware 4.30.4.a (as delivered in patch 142700-02) or later

Sun Blade 1500 Workstation (non Silver) with OBP firmware 4.30.4.a (as delivered in patch 140686-02) or later

Sun Blade 2500 Workstation (non Silver) with OBP firmware 4.30.4.a (as delivered in patch 140688-2) or later

Sun Blade 1500 Workstation Silver with OBP firmware 4.30.4.a (as delivered in patch 140687-02) or later

Sun Blade 2500 Workstation Silver with OBP firmware 4.30.4.a (as delivered in patch 140689-02) or later

Sun Fire V250 Server with OBP firmware 4.30.4.a (as delivered in patch 140688-02) or later

Sun Fire V125 Server with OBP firmware 4.30.4.a (as delivered in patch 142705-02) or later

Referencias en la web:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-276870-1>

CVEs:

Servicios (ftp, www, dns, etc.) - Vulnerabilidades de seguridad en la Transport Layer Security (TLS) y Secure Sockets Layer 3.0 (SSLv3)

Fecha: 2/10/2010

Descripción:

Una vulnerabilidad de seguridad en los protocolos TLS y SSLv3.0 durante las renegociaciones de sesión afecta a las librerías de los servicios de seguridad de red (NSS) incluidas en los productos:

- Sun Java System Web Server
- Sun Java System Web Proxy Server
- Sun Java System Application Server
- Sun GlassFish Enterprise Server
- Sun Java System Directory Server Enterprise Edition

Productos Afectados:

SPARC Platform

Sun Java System Web Server 6.1

Sun Java System Web Server 7.0 without patch 125437-18

Sun Java System Web Proxy Server 4.0 through 4.0.12 without patch 120981-20

Sun Java System Application Server 8.0 (Enterprise Edition)

Sun Java System Application Server 8.1 (Enterprise Edition SVR4) without patch 119166-40

Sun Java System Application Server 8.1 (Enterprise Edition file based) without patch 119169-33

Sun Java System Application Server 8.2 (Enterprise Edition SVR4)

Sun Java System Application Server 8.2 (Enterprise Edition file based)

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

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

x86 Platform

Sun Java System Web Server 6.1

Sun Java System Web Server 7.0 without patch 125438-18

Sun Java System Web Proxy Server 4.0 through 4.0.12 without patch 120982-20

Sun Java System Application Server 8.0 (Enterprise Edition)

Sun Java System Application Server 8.1 (Enterprise Edition SVR4) without patch 119167-40

Sun Java System Application Server 8.1 (Enterprise Edition file based) without patch 119170-33

Sun Java System Application Server 8.2 (Enterprise Edition SVR4)

Sun GlassFish Enterprise Server v2.1.1 with HADB - Package Based without patch 128641-15 (for customers with valid support contract) or 141710-03 (for customers without valid support contract)

Sun GlassFish Enterprise Server v2.1.1 with HADB without patch 128644-15 (for customers with valid support contract) or 141701-03 (for customers without valid support contract)

Linux

Sun Java System Web Server 6.1

Sun Java System Web Server 7.0 125439-16

Sun Java System Web Proxy Server 4.0 through 4.0.12

Sun Java System Application Server 8.0 (Enterprise Edition)

Sun Java System Application Server 8.1 (Enterprise Edition Package Based) without patch 119168-40

Sun Java System Application Server 8.1 (Enterprise Edition file based)

Sun Java System Application Server 8.2 (Enterprise Edition Package Based)

Sun Java System Application Server 8.2 (Enterprise Edition file based)

Sun GlassFish Enterprise Server v2.1.1 with HADB - Package Based without patch 128642-15 (for customers with valid support contract) or 141711-03 (for customers without valid support contract)

Sun GlassFish Enterprise Server v2.1.1 with HADB without patch 128645-15 (for customers with valid support contract) or 141702-03 (for customers without valid support contract)

HP-UX

Sun Java System Web Server 6.1

Sun Java System Web Server 7.0 125440-16

Sun Java System Web Proxy Server 4.0 through 4.0.12 without patch 123532-10

Windows

Sun Java System Web Server 6.1

Sun Java System Web Server 7.0 without patch 125441-18

Sun Java System Web Proxy Server 4.0 through 4.0.12 without patch 126325-10

Sun Java System Application Server 8.0 (Enterprise Edition)

Sun Java System Application Server 8.1 (Enterprise Edition Package based) without patch 122848-25

Sun Java System Application Server 8.1 (Enterprise Edition file based)

Sun Java System Application Server 8.2 (Enterprise Edition Package based)

Sun Java System Application Server 8.2 (Enterprise Edition file based)

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

and also in the following releases:

Sun Java System Directory Server 5.2 PatchZIP (Compressed Archive) Versions for Solaris 8, 9 and 10 on SPARC and x86 Platforms, Linux, Windows, HP-UX, and AIX:

Sun ONE Directory Server 5.2 without patch 142806-02

Sun Java System Directory Server Enterprise Edition PatchZIP (Compressed Archive) Versions for Solaris 9 and 10 on SPARC and x86 Platform, HP-UX, Linux, and Windows:

Sun Java System Directory Server Enterprise Edition 6.0 through 6.3.1 without patch 142807-02

Notas:

Solución:

Instalar los siguientes parches:

SPARC Platform

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 4.0.13 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 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 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 4.0.13 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 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 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 4.0.13 or later

Sun Java System Application Server 8.1 (Enterprise Edition Package Based) with patch 119168-40 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 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 4.0.13 or later

Windows

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 4.0.13 or later

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

Sistemas Operativos - Resumen de Seguridad de SUSE:

Fecha: 2/1/2010

Descripción:

En el siguiente resumen se detallan las vulnerabilidades solventadas:

- virtualbox-ose

This update of virtualbox-ose fixes a memory consumption bug in the kernel code that can be used to allocate almost all physical memory (CVE-2009-3940).

Affected Products: openSUSE 11.0, 11.1, 11.2

- NetworkManager-gnome

nm-applet connected to WPA2 Enterprise networks even if the specified CA certificate file didn't exist (CVE-2009-4144).

When editing connections in nm-applet the connection object was exported via DBus disclosing potentially sensitive information to local users (CVE-2009-4145).

Affected Products: SLE11, openSUSE 11.0, 11.1, 11.2

- avahi

The avahi-daemon reflector could cause packet storms when reflecting legacy unicast mDNS traffic (CVE-2009-0758).

Affected Products: SLE10-SP2, SLE10-SP3, SLE11, openSUSE 11.0, 11.1

- acl

the getfacl tool followed symbolic links in recursive (-R) mode even if the --physical (-P) option was specified (CVE-2009-4411).

Affected Products: SLE11, openSUSE 11.0, 11.1

- libthai

very long strings could lead to a heap buffer overflow in libthai (CVE-2009-4012).

Affected Products: SLE11, openSUSE 11.0, 11.1, 11.2

Productos Afectados:

SUSE Linux

Notas:

Referencias en la web:

http://www.novell.com/linux/security/advisories/2010_2_sr.html

CVEs:

CVE-2009-0758, CVE-2009-3940, CVE-2009-4012, CVE-2009-4144, CVE-2009-4145, CVE-2009-4411

Sistemas Operativos - Vulnerabilidad de Denegación de Servicio en Linux Kernel

Fecha: 2/5/2010

Descripción:

Se han publicado varias actualizaciones para el kernel de SUSE Linux Enterprise 10 SP2:

CVE-2009-3556: Two sysfs files in the qla2xxx driver were world writable, so users could change SCSI attributes of the qla2xxx driver.

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.

(The e1000e driver is not included in the SLES 10 SP2 kernel, so CVE-2009-4538 does not affect this kernel.)

Productos Afectados:

- SLE SDK 10 SP2
- SUSE Linux Enterprise Desktop 10 SP2
- SUSE Linux Enterprise 10 SP2 DEBUGINFO
- SUSE Linux Enterprise Server 10 SP2

Notas:

Parches a instalar:

SUSE Linux Enterprise Desktop 10 SP2 for x86

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=0e38893ae48531c465e75bb476887271

SUSE Linux Enterprise 10 SP2 DEBUGINFO for IPF

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=8e541b7f2bfe8694ff60329a4b87780b

SUSE Linux Enterprise 10 SP2 DEBUGINFO for IBM POWER

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=a02e6340cd8b95ceba636634ae907750

SLE SDK 10 SP2

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=0e38893ae48531c465e75bb476887271

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=8e541b7f2bfe8694ff60329a4b87780b

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=a02e6340cd8b95ceba636634ae907750

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=7a90bbd78c61a210fcbf21c821ac1ec8

SUSE Linux Enterprise 10 SP2 DEBUGINFO

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=0e38893ae48531c465e75bb476887271

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=8e541b7f2bfe8694ff60329a4b87780b

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=a02e6340cd8b95ceba636634ae907750

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=7a90bbd78c61a210fcbf21c821ac1ec8

SUSE Linux Enterprise Desktop 10 SP2

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=0e38893ae48531c465e75bb476887271

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=7a90bbd78c61a210fcbf21c821ac1ec8

SUSE Linux Enterprise Desktop 10 SP2 for AMD64 and Intel EM64T

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=7a90bbd78c61a210fcbf21c821ac1ec8

SUSE Linux Enterprise Server 10 SP2

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=0e38893ae48531c465e75bb476887271

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=8e541b7f2bfe8694ff60329a4b87780b

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=a02e6340cd8b95ceba636634ae907750

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=7a90bbd78c61a210fcbf21c821ac1ec8

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=1d4930dd8139d55c7a6310239ec5aacc

SUSE Linux Enterprise 10 SP2 DEBUGINFO for IBM zSeries 64bit

http://download.novell.com/index.jsp?search=Search&set_restricted=true&keywords=1d4930dd8139d55c7a6310239ec5aacc

Referencias en la web:

http://www.novell.com/linux/security/advisories/2010_09_kernel.html

CVEs:

CVE-2009-3556, CVE-2009-4536, CVE-2009-4538

Sistemas Operativos - Contenido de seguridad de iPhone OS 3.1.3 y iPhone OS 3.1.3 para iPod touch

Fecha: 2/2/2010

Descripción:

iPhone OS 3.1.3 y iPhone OS 3.1.3 para iPod touch

CoreAudio

CVE-ID: CVE-2010-0036

Disponible para: iPhone OS 1.0 hasta 3.1.2, iPhone OS para iPod touch 1.1 hasta 3.1.2

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.

ImageIO

CVE-ID: CVE-2009-2285

Disponible para: iPhone OS 1.0 hasta 3.1.2, iPhone OS para iPod touch 1.1 hasta 3.1.2

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 mejorando la comprobación de los límites.

Modo de recuperación

CVE-ID: CVE-2010-0038

Disponible para: iPhone OS 1.0 hasta 3.1.2, iPhone OS para iPod touch 1.1 hasta 3.1.2

Impacto: una persona con acceso físico a un dispositivo bloqueado podría ser capaz de acceder a los datos del usuario.

Descripción: existe un problema de corrupción de memoria causado por la gestión de un determinado mensaje de control de USB. Una persona con acceso físico al dispositivo podría aprovecharse de esta situación para eludir la contraseña y acceder a la información del usuario. Este problema se ha resuelto mejorando la gestión del mensaje de control de USB.

WebKit

CVE-ID: CVE-2009-3384

Disponible para: iPhone OS 1.0 hasta 3.1.2, iPhone OS para iPod touch 1.1 hasta 3.1.2

Impacto: el acceso a un servidor FTP creado con fines malintencionados podría conducir a la finalización inesperada de una aplicación, a la divulgación de información o a la ejecución de código arbitrario.

Descripción: existen varios problemas de validación de entrada en el manejo de listados de directorios FTP por parte de WebKit. El acceso a un servidor FTP creado con fines malintencionados podría conducir a la finalización inesperada de una aplicación, a la divulgación de información o a la ejecución de código arbitrario. Esta actualización soluciona estos problemas mejorando el análisis de los listados de directorios FTP. Gracias a Michal Zalewski, de Google Inc., por informar de estos problemas.

WebKit

CVE-ID: CVE-2009-2841

Disponible para: iPhone OS 1.0 hasta 3.1.2, iPhone OS para iPod touch 1.1 hasta 3.1.2

Impacto: Mail puede cargar contenidos de audio y vídeo remotos cuando la carga remota de imágenes está deshabilitada.

Descripción: cuando WebKit se encuentra con un Media Element HTML 5 que apunta a un recurso externo, no emite una devolución de llamada de carga de recursos para determinar si dicho recurso debería cargarse. Esto podría conducir a peticiones no deseadas a servidores remotos. Por ejemplo, el remitente de un mensaje de correo electrónico con formato HTML podría aprovecharse de esto para averiguar si el mensaje se leyó. Este problema se ha resuelto mediante la generación de devoluciones de llamada de carga de recursos cuando WebKit se encuentra con un Media Element HTML 5.

Productos Afectados:

iPhone OS 1.0 hasta 3.1.2

Notas:

Referencias en la web:

http://support.apple.com/kb/HT4013?viewlocale=es_ES

CVEs:

CVE-2010-0036, CVE-2009-2285, CVE-2010-0038 ,CVE-ID: CVE-2009-3384, CVE-2009-2841

Calle Playa de Liencres, 2
EUROPA EMPRESARIAL Edif Londres Bajo-6
Teléfono: 91 745 11 57
Fax: 91 636 63 96
28230 Las Rozas - Madrid



www.audea.com
info@audea.com