Subdirección de Seguridad de la Información - UNAM-CERT -- DGTIC-UNAM

Boletin de Seguridad UNAM-CERT-2015-001 Contenido de seguridad de OS X Yosemite v10.10.2 y actualización de seguridad 2015-001

Este documento describe el contenido de seguridad de OS X Yosemite v10.10.2 y actualización de seguridad 2015-001

- **Fecha de Liberación:** 28-Ene-2015
- **Ultima Revisión:** 9-Feb-2015
- **Fuente:**
- **CVE ID:** CVE-2011-2391 CVE-2014-1595 CVE-2014-3566 CVE-2014-3567 CVE-2014-3568 CVE-2014-4371 CVE-2014-4389 CVE-2014-4419 CVE-2014-4420 CVE-2014-4421 CVE-2014-4426 CVE-2014-4460 CVE-2014-4461 CVE-2014-4481 CVE-2014-4483 CVE-2014-4484 CVE-2014-4485 CVE-2014-4486 CVE-2014-4487 CVE-2014-4488 CVE-2014-4489 CVE-2014-4491 CVE-2014-4492 CVE-2014-4495 CVE-2014-4497 CVE-2014-4498 CVE-2014-4499 CVE-2014-6277 CVE-2014-7186 CVE-2014-7187 CVE-2014-8517 CVE-2014-8816 CVE-2014-8817 CVE-2014-8819 CVE-2014-8820 CVE-2014-8821 CVE-2014-8822 CVE-2014-8823 CVE-2014-8824 CVE-2014-8825 CVE-2014-8826 CVE-2014-8827 CVE-2014-8828 CVE-2014-8829 CVE-2014-8830 CVE-2014-8831 CVE-2014-8832 CVE-2014-8833 CVE-2014-8834 CVE-2014-8835 CVE-2014-8837 CVE-2014-8838 CVE-2014-8839
- **Riesgo** Alto
- **Problema de Vulnerabilidad** Local y remoto
- **Tipo de Vulnerabilidad** Múltiples vulnerabilidades

1. Descripción

AFP Server

- Disponible para: OS X MAvericks v10.9.5
- Impacto: Un ataque remoto que puede determinar todas las direcciones de red en el sistema.
- Descripción: El servidor de archivos APF soporta un comando el cual regresa las direcciones de red en el sistema. Esta vulnerabilidad se resolvió removiendo las direcciones del resultado.
- CVE-ID
- CVE-2014-4426: Craig Young of Tripwire VERT

bash

- Disponible para: OS X Yosemite v10.10 and v10.10.1
- Impacto: Multiples vulneravilidades en bash, incluida una que permite ataques locales de ejecucion de código arbitrario
- Descripción: Multiples vulneravilidades existentes en bash. Esta vulnerabilidad se resolvió actualizando bash para nivel de parche 57.
- CVE-ID
- CVE-2014-6277
- CVE-2014-7186
- CVE-2014-7187

Bluetooth

- Disponible para: OS X Mountain Lion v10.8.5, OS X Mavericks v10.9.5
- Impacto: Una aplicación maliciosa que puede ejecutar código arbitrario con privilegios del sistema
- Descripción: Existía un error de signo entero en IOBluetoothFamily que permite la manipulación de la memoria del kernel . Esta vulnerabilidad se resuelve mejorando la comprobación de límites. Esta vulnerabilidad no afecta a los sistemas OS X Yosemite.
- CVE-ID
- CVE-2014-4497

Bluetooth

- Disponible: OS X Yosemite v10.10 and v10.10.1
- Impacto: Una aplicación maliciosa que puede ejecutar código arbitrario con privilegios del sistema
- Descripción: Existía un error en el controlador del Bluetooth que permite la manipulación de la memoria del kernel. Esta vulnerabilidad se resuelve a través de la validación de entrada adicional.
- CVE-ID
- CVE-2014-8836 : Ian Beer of Google Project Zero

Bluetooth

- Disponible para: OS X v10.10 Yosemite y v10.10.1
- Impacto: Una aplicación maliciosa puede ser capaz de ejecutar código arbitrario con privilegios de sistema.
- Descripción: existen varios problemas de seguridad en el controlador de Bluetooth, lo que permite a una aplicación malicioso ejecutar código arbitrario con privilegios de sistema. Esta vulnerabilidad se resuelve a través de la validación de entrada adicional.
- CVE-ID
- CVE-2014-8837: Roberto Paleari and Aristide Fattori of Emaze Networks

CFNetwork caché

- Disponible para: OS X v10.10 Yosemite y v10.10.1
- Impacto: La cache del Sitio Web no se puede borrar por completo después de salir de la navegación privada
- Descripción: Los datos de navegación podrían permanecer en la memoria caché después de salir de la navegación privada. Esta vulnerabilidad se resuelve a través de un cambio en el comportamiento de la caché.
- CVE-ID
- CVE-2014-4460

CoreGraphics

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: La apertura de un archivo PDF creado de manera malintencionada puede provocar la finalización inesperada de la aplicación o la ejecución de código arbitrario
- Descripción: Existe un desbordamiento en el manejo de archivos PDF. Esta vulnerabilidad se resuelve mejorando la comprobación de límites.
- CVE-ID
- CVE-2014-4481: Felipe Andres Manzano of the Binamuse VRT, via the iSIGHT Partners GVP Program

CPU Software

- Disponible para: OS X v10.10 Yosemite y v10.10.1, para: MacBook Pro Retina, MacBook Air (mediados de 2013 y posteriores), iMac (finales de 2013 y posteriores), Mac Pro (finales de 2013)
- Impacto: Un dispositivo Thunderbolt maliciosa puede ser capaz de afectar el firmware
- Descripción: Un dispositivos Thunderbolt podría modificar el firmware de si se conecta durante una actualización EFI. Esta vulnerabilidad se resuelve al no cargar ROM opcionales durante las actualizaciones.
- CVE-ID
- CVE-2014-4498: Trammell Hudson of Two Sigma Investments

CommerceKit Framework

- Disponible para: OS X v10.10 Yosemite y v10.10.1
- Impacto: Un atacante con acceso a un sistema puede ser capaz de recuperar las credenciales de identificación de Apple
- Descripción: Un problema existía en el manejo de los registros de la App Store. El proceso de la App Store podía registrar credenciales de identificación de Apple en el registro cuando el registro adicional fue habilitada. Esta vulnerabilidad se resuelve no permitir el registro de las credenciales.
- CVE-ID
- CVE-2014-4499: Sten Petersen

CoreGraphics

- Disponible para: OS X v10.10 Yosemite y v10.10.1
- Impacto: Algunas aplicaciones de terceros con eventos no seguros de entrada de texto y el uso del ratón.
- Descripción: Debido a la combinación de una variable no inicializada y de asignado de memoria de una aplicación, eventos de entrada de texto y el ratón no seguras pueden haber sido registrados. Esta vulnerabilidad se resuelve garantizando que el registro está desactivado por defecto. Esta vulnerabilidad no afecta a los sistemas anteriores a OS X Yosemite.
- CVE-ID
- CVE-2014-1595: Steven Michaud of Mozilla working with Kent Howard

CoreGraphics

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks
- Impacto: La apertura de un archivo PDF creado de manera malintencionada puede provocar la finalización inesperada de la aplicación o la ejecución de código arbitrario
- Descripción: Problema de corrupción de memoria existente en el manejo de archivos PDF. Esta vulnerabilidad se resuelve se resuelve mejorando la comprobación de límites. Esta vulnerabilidad no afecta a los sistemas OS X Yosemite.
- CVE-ID
- CVE-2014-8816: Mike Myers, of Digital Operatives LLC

CoreSymbolication

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: Una aplicación maliciosa puede ser capaz de ejecutar código arbitrario con privilegios de sistema
- Descripción: Múltiples problemas de confusión de tipo existió en el manejo de coresymbolicationd (proceso propio de OS X) de mensajes XPC. Esta vulnerabilidad se resuelve a través de la mejora de la comprobación de tipos.
- CVE-ID

- CVE-2014-8817: Ian Beer of Google Project Zero

FontParser

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: El procesamiento de un archivo .dfont con fines malintencionados puede provocar la finalización inesperada de la aplicación o la ejecución de código arbitrario.
- Descripción: Un problema de corrupción de memoria existente en el manejo de archivos .dfont. Eta vulnerabilidad se resuelve mejorando la comprobación de límites.
- CVE-ID
- CVE-2014-4484: Gaurav Baruah working with HP's Zero Day Initiative

FontParser

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: La apertura de un archivo PDF creado de manera malintencionada puede provocar la finalización inesperada de la aplicación o la ejecución de código arbitrario
- Descripción: existe un desbordamiento de búfer en el manejo de los archivos fuente. Esta vulnerabilidad se resuelve mejorando la comprobación de límites.
- CVE-ID
- CVE-2014-4483: Apple

Foundation

- Disponible para: OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: La visualización de un archivo XML con fines malintencionados puede provocar la finalización inesperada de la aplicación o la ejecución de código arbitrario
- Descripción: Existe un desbordamiento de búfer en el analizador XML. Esta vulnerabilidad se resuelve mejorando la comprobación de límites.
- CVE-ID
- CVE-2014-4485: Apple

Intel Graphics Driver

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: múltiples vulnerabilidades en el controlador gráfico de Intel
- Descripción: Múltiples vulnerabilidades existían en el controlador de gráficos Intel, el más grave de lo que puede haber dado lugar a la ejecución de código arbitrario con privilegios de sistema. Esta actualización resuelve los problemas a través de comprobaciones adicionales.
- CVE-ID
- CVE-2014-8819: Ian Beer of Google Project Zero
- CVE-2014-8820: Ian Beer of Google Project Zero
- CVE-2014-8821: Ian Beer of Google Project Zero

IOAcceleratorFamily

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: Una aplicación maliciosa puede ser capaz de ejecutar código arbitrario con privilegios de sistema
- Descripción: Existía una referencia a un puntero nulo en el manejo de IOAcceleratorFamily de ciertos tipos de clientes IOService. Esta vulnerabilidad se soluciona mejorando la validación de los contextos IOAcceleratorFamily.

- CVE-ID
- CVE-2014-4486: Ian Beer of Google Project Zero

IOHIDFamily

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: Una aplicación maliciosa puede ser capaz de ejecutar código arbitrario con privilegios de sistema
- Descripción: existe un desbordamiento de búfer en IOHIDFamily. Esta vulnerabilidad se resuelve con la mejora de la comprobación de límites.
- CVE-ID
- CVE-2014-4487: Taig Jailbreak Team

IOHIDFamily

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: Una aplicación maliciosa puede ser capaz de ejecutar código arbitrario con privilegios de sistema
- Descripción: Un problema de validación existía en el manejo de IOHIDFamily de metadatos de los recursos. Esta vulnerabilidad se soluciona mejorando la validación de los metadatos.
- CVE-ID
- CVE-2014-4488: Apple

IOHIDFamily

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: Una aplicación maliciosa puede ser capaz de ejecutar código arbitrario con privilegios de sistema
- Descripción: Existía una referencia a un puntero nulo en el manejo de IOHIDFamily de colas de eventos. Esta vulnerabilidad se soluciona mejorando la validación de IOHIDFamily inicialización cola de eventos.
- CVE-ID
- CVE-2014-4489: @beist

IOHIDFamily

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: La ejecución de una aplicación maliciosa puede provocar la ejecución de código arbitrario en el kernel
- Descripción: Una cuenta de comprobación en un cliente expendido por el controlador IOHIDFamily que permitió a una aplicación maliciosa sobrescribir porciones arbitrarias del espacio de direcciones del kernel. La vulnerabilidad se soluciona quitando el método de cliente vulnerable.
- CVE-ID
- CVE-2014-8822: Vitaliy Toropov working with HP's Zero Day Initiative

IOKit

- Disponible para: OS X v10.10 Yosemite y v10.10.1
- Impacto: Una aplicación maliciosa puede ser capaz de ejecutar código arbitrario con privilegios de sistema

- Descripción: Existe un desbordamiento en el manejo de las funciones IOKit. Esta vulnerabilidad se soluciona mejorando la validación de argumentos API IOKit.
- CVE-ID
- CVE-2014-4389: Ian Beer of Google Project Zero

IOUSBFamily

- Disponible para: OS X v10.10 Yosemite y v10.10.1
- Impacto: Una aplicación privilegiada puede ser capaz de leer datos arbitrarios de la memoria del Kernel
- Descripción: un problema de acceso a memoria existía en el manejo de las funciones del cliente del controlador IOUSB. Esta vulnerabilidad se soluciona mejorando la validación de argumentos.
- CVE-ID
- CVE-2014-8823: Ian Beer of Google Project Zero

Kernel

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: Una aplicación maliciosa puede ser capaz de ejecutar código arbitrario con privilegios de sistema
- Descripción: Especificación de un modo de caché personalizado permitio escribir en el kernel segmentos de memoria de sólo lectura compartidos. Esta vulnerabilidad se resuelve la no conceder permisos de escritura como un efecto secundario de algunos modos de caché personalizado.
- CVE-ID
- CVE-2014-4495: Ian Beer of Google Project Zero

Kernel

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: Una aplicación maliciosa puede ser capaz de ejecutar código arbitrario con privilegios de sistema
- Descripción: Un problema de validación existía en el manejo de ciertos campos de metadatos de los objetos IODataQueue. Esta vulnerabilidad se soluciona mejorando la validación de los metadatos.
- CVE-ID
- CVE-2014-8824:PanguTeam

Kernel

- Disponible para: OS X v10.10 Yosemite y v10.10.1
- Impacto: Un atacante local puede suplantar las respuestas del servicio de directorio para el kernel, elevar los privilegios, o ganar la ejecución del kernel
- Descripción: Existían vulnerabilidades en la validación identitysvc del proceso de resolución de servicio de directorio, el manejo de la bandera y en el tratamiento de errores. Esta vulnerabilidad se soluciona mejorando la validación.
- CVE-ID
- CVE-2014-8825: Alex Radocea of CrowdStrike

Kernel

- Disponible para: OS X v10.10 Yosemite y v10.10.1
- Impacto: un usuario local puede ser capaz de determinar el diseño de memoria del kernel

- Descripción: Múltiples problemas de memoria sin inicializar existían en la interfaz de estadísticas de la red, lo que dio lugar a la divulgación del contenido de la memoria del Kernel. Esta cuestión fue tratada mediante la inicialización de memoria adicional.
- CVE-ID
- CVE-2014-4371: Fermin J. Serna of the Google Security Team
- CVE-2014-4419: Fermin J. Serna of the Google Security Team
- CVE-2014-4420: Fermin J. Serna of the Google Security Team
- CVE-2014-4421: Fermin J. Serna of the Google Security Team

Kernel

- Disponible para: OS X v10.9.5 Mavericks
- Impacto: Una persona con una posición privilegiada en la red puede causar una denegación de servicio
- Descripción: Un problema en el manejo de paquetes IPv6.Esta vulnerabilidad se soluciona mejorando la comprobación de estado de bloqueo.
- CVE-ID
- CVE-2011-2391

Kernel

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: Las aplicaciones con fines malintencionados o comprometidos pueden ser capaces de determinar las direcciones en el kernel
- Descripción: Un problema de divulgación de información existente en el manejo de las API relacionadas con las extensiones del kernel. Las respuestas contienen una clave OSBundleMachOHeaders que pueden haber incluido direcciones del Kernel, que pueden ayudar para pasar por la protección del espacio de direcciones aleatorias. Esta vulnerabilidad se resolvió evitando el desplazamiento de las direcciones antes de devolverlas.
- CVE-ID
- CVE-2014-4491: @PanguTeam, Stefan Esser

Kernel

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: Una aplicación maliciosa puede ser capaz de ejecutar código arbitrario con privilegios de sistema
- Descripción: Un problema de validación existía en el manejo de ciertos campos de metadatos de los objetos IOSharedDataQueue. Esta vulnerabilidad se resolvió a través de la reubicación de los metadatos.
- CVE-ID
- CVE-2014-4461: @PanguTeam

LaunchServices

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: un archivo JAR malicioso puede omitir las comprobaciones de Gatekeeper
- Descripción: un problema existía en el manejo de inicialización de aplicaciones que permitían a ciertos archivos JAR maliciosos burlar los controles de Gatekeeper. Esta vulnerabilidad se soluciona mejorando la gestión del tipo de archivo de metadatos.
- CVE-ID
- CVE-2014-8826: Hernan Ochoa of Amplia Seguridad

Libnetcore

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: Una aplicación sandboxed malicioso puede comprometer el demonio networkd
- Descripción: Múltiples problemas de confusión existió en el manejo de networkd de comunicación entre procesos. Mediante el envío de un mensaje networkd maliciosamente formateado, puede que haya sido posible ejecutar código arbitrario como el proceso networkd. Esta vulnerabilidad se resuelve mediante la comprobación de tipos adicional.
- CVE-ID
- CVE-2014-4492: Ian Beer of Google Project Zero

LoginWindow

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: Un Mac no puede bloquearse inmediatamente después de iniciar
- Descripción: un problema existía en la prestación de la pantalla de bloqueo. Esta vulnerabilidad se resuelve mediante una mejor visualización en pantalla mientras está bloqueado.
- CVE-ID
- CVE-2014-8827: Xavier Bertels of Mono, and multiple OS X seed testers

lukemftp

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: el uso de la herramienta de línea de comandos ftp al buscar archivos de un servidor http malicioso puede provocar la ejecución de código arbitrario
- Descripción: un problema de inyección de comandos existía en el manejo de redirecciones HTTP. Esta vulnerabilidad se soluciona mejorando la validación de caracteres especiales.
- CVE-ID
- CVE-2014-8517

OpenSSL

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: múltiples vulnerabilidades en OpenSSL 0.9.8za, incluyendo uno que podría permitir a un atacante de degradar las conexiones para utilizar suites de cifrado más débiles en aplicaciones utilizando la biblioteca
- Descripción: Múltiples vulnerabilidades existían en OpenSSL 0.9.8za. Esta vulnerabilidad se resolvió mediante la actualización a la versión de OpenSSL 0.9.8zc.
- CVE-ID
- CVE-2014-3566
- CVE-2014-3567
- CVE-2014-3568

Sandbox

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks
- Impacto: un proceso de espacio aislado puede ser capaz de eludir las restricciones de una Sandbox
- Descripción: un problema de diseño existía en el almacenamiento en caché de perfiles sandbox que permitió aplicaciones de espacio aislado para tener acceso de escritura a la

memoria caché. Esta vulnerabilidad se resolvió con la restricción de acceso de escritura a rutas que contienen un segmento "com.apple.sandbox". Esta vulnerabilidad no afecta a v10.10 OS X Yosemite o posterior.
- CVE-ID
- CVE-2014-8828: Apple

SceneKit

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks
- Impacto: Una aplicación maliciosa podría ejecutar código arbitrario que compromete la información de usuario
- Descripción: Múltiples vulnerabilidades de límites escritura existía en SceneKit. Estos temas fueron abordados a través de la mejora de la comprobación de límites.
- CVE-ID
- CVE-2014-8829: Jose Duart of the Google Security Team

SceneKit

- Disponible para: OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: la visualización de un archivo Collada con fines malintencionados puede provocar la finalización inesperada de la aplicación o la ejecución de código arbitrario
- Descripción: existe un desbordamiento del búfer de montones cuando SceneKit de archivos Collada. Ver un archivo Collada fines malintencionados puede haber dado lugar a una terminación inesperada de la aplicación o la ejecución de código arbitrario. Esta vulnerabilidad se soluciona mejorando la validación de elementos de descriptor de acceso.
- CVE-ID
- CVE-2014-8830: Jose Duart of Google Security Team

Security

- Disponible para: OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: una aplicación descargada y firmada con un certificado de ID de desarrollador revocado puede pasar los chequeos de Gatekeeper
- Descripción: un problema existía con la forma en caché de la información de certificados. Esta vulnerabilidad se soluciono con mejoras en las lógicas de la cache.
- CVE-ID
- CVE-2014-8838: Apple

Security_taskgate

- Disponible para: OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: Una aplicación puede acceder a los elementos del llavero perteneciente a otras aplicaciones
- Descripción: un problema de control de acceso existente en el llavero. Las aplicaciones firmadas con certificados de identificación con firma o desarrollador puede acceder a los elementos llavero cuyo control de acceso se basan en grupos llavero. Esta vulnerabilidad se soluciono mediante la validación de la identidad de la firma en la concesión de acceso a los grupos llavero.
- CVE-ID
- CVE-2014-8831: Apple

Spotlight

- Disponible para: OS X v10.10 Yosemite y v10.10.1
- Impacto: El remitente de un correo electrónico podría determinar la dirección IP del destinatario

- Descripción: Spotlight no comprobó el estado de "contenido remoto de carga en los mensajes" del correo de ajuste. Esta vulnerabilidad se soluciono mediante la mejora de la comprobación de la configuración.
- CVE-ID
- CVE-2014-8839: John Whitehead of The New York Times, Frode Moe of LastFriday.no

Spotlight

- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: Spotlight puede guardar información inesperada en un disco duro externo
- Descripción: un problema existía en Spotlight, el contenido de la memoria podía ser escrito para discos duros externos en la indexación. Esta vulnerabilidad se soluciono una mejor gestión de la memoria.
- CVE-ID
- CVE-2014-8832: F-Secure

SpotlightIndex

- Disponible para: OS X v10.10 Yosemite y v10.10.1
- Impacto: Spotlight puede mostrar los resultados de ficheros que no pertenecen al usuario
- Descripción: un problema de serialización existía en el manejo de Spotlight en la cache de permisos. Un usuario que realiza una consulta de Spotlight puede mostrar resultados de búsqueda que hacen referencia a archivos para los que no tienen suficientes privilegios para leer. Esta vulnerabilidad se soluciono mejora de la comprobación de límites.
- CVE-ID
- CVE-2014-8833: David J Peacock, Independent Technology Consultant

Sysmond

- Disponible para: OS X v10.9.5 Mavericks, OS X v10.10 Yosemite y v10.10.1
- Impacto: Una aplicación maliciosa puede ser capaz de ejecutar código arbitrario con privilegios de root
- Descripción: existe una vulnerabilidad de tipo confusión en sysmond que permitió una aplicación local escalar privilegios. Esta vulnerabilidad se soluciono con la mejora de la comprobación de tipos.
- CVE-ID
- CVE-2014-8835: Ian Beer of Google Project Zero

UserAccountUpdater

- Disponible para: OS X v10.10 Yosemite y v10.10.1
- Impacto: los archivos relacionadas con la Impresión puede contener información sensible acerca de los documentos PDF
- Descripción: OS X Yosemite v10.10 abordan un problema en el manejo de archivos PDF protegidos por contraseña creados a partir del momento de Imprimir donde las contraseñas pueden haber sido incluidos en los archivos de preferencias de impresión. Esta actualización elimina tal información extraña que pueda haber estado presente en las preferencias de impresión.
- CVE-ID
- CVE-2014-8834: Apple

2. Referencias

http://support.apple.com/en-us/HT204244

La Subdirección de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Manuel Ignacio Quintero Martínez (mquintero at seguridad dot unam dot mx)
- Jose Carmen Hernandez Padron (jhernandez at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Subdirección de Seguridad de la Información

incidentes at seguridad.unam.mx
phishing at seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 47