Boletin de Seguridad UNAM-CERT-2015-004 OS X Yosimete v10.10.2 y actualización de seguridad 2015-001

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

- **Fecha de Liberación:** 27-Ene-2015
- **Ultima Revisión:** 9-Feb-2015
- **Fuente:**
- **CVE ID:** CVE-2014-1595 CVE-2014-3566 CVE-2014-3567 CVE-2014-3568 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-2014-8836 CVE-2014-8837 CVE-2014-8838 CVE-2014-8839
- **Riesgo** Muy Alto
- **Problema de Vulnerabilidad** Local y remoto
- **Tipo de Vulnerabilidad** Ejecución Remota de Código

1. Descripción

AFP Server

- Disponible para: OS X Mavericks v10.9.5
- Impacto: un atacante de manera remota podría determinar todas las direcciones de red del sistema.
- Descripción: El servidor de archivos AFP soporta un comando que responde con todas las direcciones de red del sistema. Esta vulnerabilidad fue tratada eliminando las direcciones en el resultado.
- CVE-2014-4426

bash

- Disponible para: OS X Yosemite v10.10 and v10.10.1
- Impacto: Múltiples vulnerabilidades en bash, incluyendo una que permite a los atacantes ejecutar código arbitrario de manera local.
- Múltiples vulnerabilidades existen en bash. Estas vulnerabilidades se resolvieron al actualizar el bash con el parche nivel 57.
- 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 podría ejecutar código arbitrario con privilegios del sistema.
- Existe un error de signo entero en IOBluetoothFamily el cual permite la manipulación de la memoria del kernel. Esta vulnerabilidad se resolvió mejorando la comprobación de límites. Esta vulnerabilidad no afecta el sistema OS X Yosimite.
- CVE-2014-4497

Bluetooth

- Disponible para: OS X Yosemite v10.10 and v10.10.1
- Una aplicación maliciosa podría ejecutar código arbitrario con privilegios del sistema.
- Existe un error en el controlador de Bluettooth, que permite a una aplicación maliciosa controlar el tamaño de escritura en la memoria del kernel. Esta vulnerabilidad se resolvió con validaciones adicionales de entrada.
- CVE-2014-8836 : Ian Beer of Google Project Zero

Bluetooth

- Disponible para: OS X Yosemite v10.10 and v10.10.1
- Una aplicación maliciosa podría ejecutar código arbitrario con privilegios del sistema.
- Existen múltiples vulnerabilidades de seguridad en el controlador de Bluetooth, que permiten a una aplicación maliciosa ejecutar código arbitrario con privilegios del sistema. Esta vulnerabilidad se resolvió con validaciones adicionales de entrada.
- 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 en Website no se puede borrar por completo después de salir de la navegación privada.
- Descripción: Existe una vulnerabilidad donde los datos de navegación podrían permanecer en la memoria caché después de salir de la navegación privada. Esta vulnerabilidad se resolvió con un cambio en el comportamiento de la caché.
- 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: Abrir un archivo PDF creado de manera malintencionada puede provocar la finalización inesperada de la aplicación o ejecución de código arbitrario.
- Descripción: existe un desbordamiento de enteros en la manera en que se manejan archivos PDF. Esta vulnerabilidad se resolvió mejorando la comprobación de límites.
- CVE-2014-4481: Felipe Andrés Manzano del Binamuse VRT, a través del Programa de Partners iSIGHT GVP

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 malicioso de Thunderbolt podría afectar el firmware flashing.
- Descripción: Los dispositivos Thunderbolt podrían modificar el firmware si es conectado durante una actualización de EFI. Esta vulnerabilidad se resolvió al no cargar las opciones de ROM durante las actualizaciones.

- CVE-2014-4498: Trammell Hudson de Inversiones Dos Sigma

CommerceKit Framework

- Disponible para: OS X v10.10 Yosemite y v10.10.1
- Impacto: Un atacante con acceso a un sistema podría recuperar las credenciales de Apple ID.
- Descripción: Existe una vulnerabilidad en el manejo de los registros de App Store. El proceso de App Store podría registrar el Apple ID cuando un registro adicional se encuentra habilitado. Esta vulnerabilidad se resolvió al no permitir el registro de las credenciales.
- CVE-2014-4499: Sten Petersen

CoreGraphics

- Disponible para: OS X v10.10 Yosemite y v10.10.1
- Impacto: Algunas aplicaciones de terceros con eventos de entrada de texto y ratón no seguras podrían conectarse a dichos eventos.
- Descripción: Debido a la combinación de una variable no inicializada y un apuntador personal a una aplicación, además de eventos de entrada de texto y el ratón no seguras podrían ser registrados. Esta vulnerabilidad se resolvió garantizando que el registro está desactivado de manera predeterminada. Esta vulnerabilidad no afecta a los sistemas anteriores a OS X Yosemite.

CVE-2014-1595: Steven Michaud de Mozilla trabajar con Kent Howard

- CoreGraphics
- Disponible para: OS X Mountain Lion v10.8.5, OS X v10.9.5 Mavericks
- Impacto: Al abrir un archivo PDF creado de manera malintencionada puede provocar la finalización inesperada de la aplicación o ejecución de código arbitrario.
- Descripción: Existe una vulnerabilidad de corrupción de memoria en el manejo de archivos PDF. Esta vulnerabilidad se resuelve mejorando la comprobación de límites. Esta vulnerabilidad no afecta a los sistemas OS X Yosemite.
- CVE-2014-8816: Mike Myers, de digital Operarios 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 podría ejecutar código arbitrario con privilegios de sistema.
- Descripción: Existen múltiples vulnerabilidades de confusión en el manejo de de mensajes de coresymbolicationd de XPC. Estas vulnerabilidades se resolvieron mejorando la comprobación de tipos de mensajes.
- CVE-2014-8817: Ian Beer de 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 maliciosos puede provocar la finalización inesperada de la aplicación o la ejecución de código arbitrario.
- Descripción: Existe una vulnerabilidad de corrupción de memoria en el manejo de archivos .dfont. Esta vulnerabilidad se resolvió mejorando la comprobación de límites.
- CVE-2014-4484: Gaurav Baruah trabajando con Zero Day Initiative de HP

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:
- Abrir 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 del buffer en el manejo de archivos fuente. Esta vulnerabilidad se resolvió mejorando la comprobación de límites.
- 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 maliciosos puede provocar la finalización inesperada de la aplicación o la ejecución de código arbitrario
- Descripción: Existe un desbordamiento de buffer en el analizador XML. Esta vulnerabilidad se resolvió mejorando la comprobación de límites.
- 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: Existen múltiples vulnerabilidades en el controlador de gráficos de Intel. Descripción: Existen múltiples vulnerabilidades en el controlador de gráficos de Intel, la más grave de estas vulnerabilidades puede permtir la ejecución de código arbitrario con privilegios del sistema. Esta actualización se resolvió a con comprobación adicional de límites.
- CVE-2014-8819: Ian Beer de Google Project Zero
- CVE-2014-8820: Ian Beer de Google Project Zero
- CVE-2014-8821: Ian Beer de 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 podría de ejecutar código arbitrario con privilegios de sistema.
- Descripción: Existía una referencia a un puntero nulo en el manejo de IOAcceleratorFamily de ciertos tipos userclient en IOService. Este problema se resolvió mejorando la validación de los contextos en IOAcceleratorFamily.
-
- CVE-2014-4486: Ian Beer de 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 podría de ejecutar código arbitrario con privilegios de sistema.
- Descripción: Existe un desbordamiento de buffer en IOHIDFamily. Esta vulnerabilidad se resolvió con la mejora de la comprobación de límites.
- CVE-2014-4487: Taig Jailbreak Equipo

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 podría ejecutar código arbitrario con privilegios de sistema.
- Descripción: Existe una vulnerabilidad en el manejo de validación de metadatos de los recursos de IOHIDFamily. Esta vulnerabilidad se resolvió mejorando la validación de los metadatos.
- 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 podría ejecutar código arbitrario con privilegios de sistema.
- Descripción: Existe una vulnerabilidad a un apuntador nulo en el manejo de colas de eventos en IOHIDFamily. Esta vulnerabilidad se resolvió mejorando la validación de inicialización de cola de eventos de IOHIDFamily.
-
- 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: Existe una vulnerabilidad en la comprobación de un cliente usuario emitido por el controlador de IOHIDFamily que permite a una aplicación maliciosa sobrescribir porciones arbitrarias en el espacio de direcciones del kernel. La vulnerabilidad se resolvió quitando el método de cliente usuario vulnerable.
- CVE-2014-8822: Vitaliy Toropov trabajando con Zero Day Initiative de HP

IOKit

- Disponible para: OS X v10.10 Yosemite y v10.10.1
- Impacto: Una aplicación maliciosa podría ejecutar código arbitrario con privilegios de sistema.
- Descripción: Existe un desbordamiento de enteros en el manejo de las funciones de IOKit. Esta vulnerabilidad se resolvió mejorando la validación de argumentos API IOKit.
- CVE-2014-4389: Ian Beer de Google Project Zero

IOUSBFamily

- Disponible para: OS X v10.10 Yosemite y v10.10.1
- Impacto: Una aplicación privilegiada podría leer datos arbitrarios de la memoria del kernel.
- Descripción: Existe una vulnerabilidad de acceso a memoria por el controlador de IOUSB en el manejo de las funciones del usuario. Esta vulnerabilidad se resolvió mejorando la validación de argumentos.
- CVE-2014-8823: Ian Beer de 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 podría de ejecutar código arbitrario con privilegios de sistema
- Descripción: Especificación de un modo de caché personalizado permitido escribir al kernel segmentos de memoria de sólo lectura compartidos. Esta vulnerabilidad se resolviópor la no concesión de permisos de escritura como un efecto secundario de algunos modos de caché personalizado.
- CVE-2014-4495: Ian Beer de 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 podría de ejecutar código arbitrario con privilegios de sistema.
- Descripción: Existe una vulnerabilidad de validación en el manejo de ciertos campos de metadatos de los objetos IODataQueue. Esta vulnerabilidad se resolvió mejorando la validación de los metadatos.
- 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 beneficiarse de la ejecución del kernel.
- Descripción: Existe una vulnerabilidad en la validación de identitysvc durante el proceso de resolución de servicio de directorio, manejo de banderas y tratamiento de errores. Esta vulnerabilidad se resolvió mejorando la validación.
- CVE-2014-8825: Alex Radocea de CrowdStrike

Kernel

- Disponible para: OS X v10.10 Yosemite y v10.10.1
- Impacto: Un usuario local podría de determinar el diseño de memoria del kernel.
- Descripción: Existen múltiples vulnerabilidades de memoria sin inicializar en la interfaz de estadísticas de la red, lo que da lugar a la divulgación del contenido de la memoria del kernel. Esta vulnerabilidad se resolvió mediante la inicialización de memoria adicional.
- CVE-2014-4371: Fermín J. Serna del equipo de seguridad de Google
- CVE-2014-4419: Fermín J. Serna del equipo de seguridad de Google
- CVE-2014-4420: Fermín J. Serna del equipo de seguridad de Google
- CVE-2014-4421: Fermín J. Serna del equipo de seguridad de Google

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: Existe una vulnerabilidad en el manejo de paquetes IPv6. Esta vulnerabilidad se resolvió mejorando la comprobación de estado de bloqueo.
- 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 maliciosos o comprometidas pueden ser capaces de determinar las direcciones en el kernel.

- Descripción: Existe una vulnerabilidad de divulgación de información por el manejo de las API relacionadas con las extensiones del kernel. Las respuestas contienen una clave OSBundleMachOHeaders que pueden haber incluido direcciones del kernel, además de ayudar a pasar por la protección del espacio de direcciones aleatoria del diseño. Esta vulnerabilidad se resolvió quitando el desplazamiento de direcciones antes de devolverlas.
- 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 podría ejecutar código arbitrario con privilegios de sistema.
- Descripción: Existe una vulnerabilidad de validación en el manejo de ciertos campos de metadatos de los objetos IOSharedDataQueue. Esta vulnerabilidad se resolvió con la reubicación de los metadatos.
- 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: Existe una vulnerabilidad en el manejo de lanzamiento de aplicaciones que permite a ciertos archivos JAR maliciosos omitir los controles de Gatekeeper. Esta vulnerabilidad se resolvió mejorando la gestión del tipo de archivo de metadatos.
- CVE-2014-8826: Hernán Ochoa de 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 sandboxed maliciosa puede comprometer el demonio networkd.
- Descripción: Existen múltiples vulnerabilidades de confusión de tipo en el manejo de comunicación entre procesos networkd. Mediante el envío de un mensaje malicioso de networkd, puede ser que haya sido posible ejecutar código arbitrario como el proceso networkd. El problema se resuelve mediante la comprobación de tipos adicional.
- CVE-2014-4492: Ian Beer de 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 se puede bloquear inmediatamente después de salir de modo de espera.
- Descripción: Existe una vulnerabilidad en la presentación de la pantalla de bloqueo. Esta vulnerabilidad era una dirección que permitía una mejor visualización en pantalla mientras está bloqueada.
- CVE-2014-8827: Xavier Bertels de Mono, y varios certificadores de semillas OS X

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 podría permitir la ejecución de código arbitrario

- Descripción: Existe una vulnerabilidad de inyección de comandos en el manejo de redirecciones HTTP. Esta vulnerabilidad se resolvió mejorando la validación de caracteres especiales.
- 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 bajar las conexiones para utilizar las suites de cifrado más débiles en aplicaciones utilizando una biblioteca.
- Descripción: Múltiples vulnerabilidades existían en OpenSSL 0.9.8za.. Estas vulnerabilidades se resolvieron con la actualización a la última versión de OpenSSL 0.9.8zc.
-
- 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 podría omitir las restricciones de la sandbox.
- Descripción: Existe una vulnerabilidad de diseño en el almacenamiento de perfiles en caché de la sandbox que permite a aplicaciones tener acceso de escritura a la memoria caché. Esta vulnerabilidad se resolvió mediante 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-2014-8828: Apple

SceneKit

- Disponible para: OS X Mountain Lion v10.8.5, OS X Mavericks v10.9.5
- Impacto: Una aplicación maliciosa podría ejecutar código arbitrario que lleva comprometida la información de usuario.
- Descripción: Múltiples vulnerabilidades fuera de límite pueden escribir en SceneKit. Estas vulnerabilidades fueron resueltas a través de la mejora de la comprobación de límites.
- CVE-2014-8829 : Jose Duart of the Google Security Team

SceneKit

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

Security

- Disponible para: OS X Mavericks v10.9.5, OS X Yosemite v10.10 y v10.10.1
- Impacto: Una aplicación descargada y firmada con un certificado de ID Desarrollado revocado puede pasar cheques Gatekeeper.

- Descripción: Existe una vulnerabilidad con la forma de certificados aplicación en caché. Esta vulnerabilidad fue resuelta con mejoras lógicas caché.
- CVE-2014-8838 : Apple

security_taskgate

- Disponible para: OS X Mavericks v10.9.5, OS X Yosemite v10.10 y v10.10.1
- Impacto: Una aplicación puede acceder a los elementos llavero pertenecientes a otras aplicaciones.
- Descripción: Existe una vulnerabilidad de control de acceso existente en el llavero. Las aplicaciones firmadas con certificados de identificación con firma pueden acceder a los elementos llavero cuyas listas de control de acceso se basan en grupos llavero. Esta vulnerabilidad fue resuelta mediante la validación de la identidad de la firma en la concesión de acceso a los grupos llavero.
- CVE-2014-8831 : Apple

Spotlight

- Disponible para: OS X Yosemite v10.10 y v10.10.1
- Impacto: El remitente de un correo electrónico podría determinar la dirección IP del destinatario.
- Descripción: Spotlight no comprueba el estado de "contenido remoto de carga en los mensajes" del correo de ajuste. Esta vulnerabilidad fue resuelta mediante la mejora de la comprobación de la configuración.
- CVE-2014-8839 : John Whitehead de The New York Times, Frode Moe de LastFriday.no

Spotlight

- Disponible para: OS X Mountain Lion v10.8.5, OS X Mavericks v10.9.5, OS X Yosemite v10.10 y v10.10.1
- Impacto: Spotlight puede guardar información de manera inesperada en un disco duro externo.
- Descripción: Existe una vulnerabilidad en Spotlight donde el contenido de la memoria puede ser escrito para discos duros externos cuando hay indexación. Esta vulnerabilidad fue resuelta con una mejor gestión de la memoria.
- CVE-2014-8832 : F-Secure

SpotlightIndex

- Disponible para: OS X Yosemite v10.10 y v10.10.1
- Impacto: Spotlight puede mostrar los resultados de los archivos que no pertenecen al usuario.
- Descripción: Existe una vulnerabilidad no seriada en el manejo de permisos en caché de Spotlight. Un usuario que realiza una consulta de Spotlight puede mostrar resultados de búsqueda que hacen referencia a archivos que no tiene privilegios para leer. Esta vulnerabilidad fue resuelta con la mejora de la comprobación de límites.
- CVE-2014-8833 : David J Peacock, Independent Technology Consultant

sysmond

- Disponible para: OS X Mavericks v10.9.5, OS X Yosemite v10.10 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 permite a una aplicación local escalar privilegios. La vulnerabilidad fue resuelta con la mejora de la comprobación de tipos.
- CVE-2014-8835 : Ian Beer of Google Project Zero

UserAccountUpdater

- Disponible para: OS X Yosemite v10.10 y v10.10.1
- Impacto: Los archivos de preferencias relacionados con la impresión pueden contener información sensible acerca de los documentos PDF.
- Descripción: OS X Yosemite v10.10 solucionó una vulnerabilidad en el manejo de archivos PDF protegidos por contraseña creados a partir del diálogo Imprimir donde las contraseñas pueden ser incluidas en los archivos de preferencias de impresión. Esta actualización elimina la información extraña que pueda estar presente en la impresión de archivos de preferencias.
- CVE-2014-8834 : Apple

2. Referencias

- http://support.apple.com/en-us/HT1222
- 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:

- Edgar Israel Rubi Chavez (erubi at seguridad dot unam dot mx)
- Manuel Ignacio Quintero Martínez (mquintero 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