Boletin de Seguridad UNAM-CERT-2015-003 Contenido de Seguridad iOS 8.1.3

Este documento describe el contenido de seguridad relacionado con iOS 8.1.3

- **Fecha de Liberación:** 27-Ene-2015
- **Ultima Revisión:** 6-Feb-2015
- **Fuente:**
- **CVE ID:** CVE-2014-3192 CVE-2014-4455 CVE-2014-4459 CVE-2014-4465 CVE-2014-4466 CVE-2014-4467 CVE-2014-4468 CVE-2014-4469 CVE-2014-4470 CVE-2014-4471 CVE-2014-4472 CVE-2014-4473 CVE-2014-4474 CVE-2014-4475 CVE-2014-4476 CVE-2014-4477 CVE-2014-4479 CVE-2014-4480 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-2014-4493 CVE-2014-4494 CVE-2014-4495 CVE-2014-4496 CVE-2014-8840 VU#275289
- **Riesgo** Alto
- **Problema de Vulnerabilidad** Local y remoto
- **Tipo de Vulnerabilidad** Múltiples vulnerabilidades

1. Descripción

AppleFileConduit

- Disponible para: iPhone 4s y posterior, iPod touch (5ta generación) y posterior, iPad 2 y posterior
- Impacto: Un comando malicioso afc especialmente diseñado podría permitir el acceso a partes protegidas del sistema de archivos.
- Descripción: Existe una vulnerabilidad en el mecanismo de ligas simbólicas de afc. Esta vulnerabilidad se resolvió añadiendo controles de ruta adicionales.
- CVE-2014-4480 : TaiG Jailbreak Team

CoreGraphics

- Disponible para: iPhone 4s y posteriores, iPod touch (5ta generación) y posteriores, iPad 2 y posteriores.
- Impacto: Abrir un archivo PDF maliciosos especialmente diseñado puede llevar a un cierre de aplicaciones inesperado o a la ejecución arbitraria de código.
- Descripción: Existe un desbordamiento de enteros en el manejador de archivos PDF. Esta vulnerabilidad se resolvió mejorando la comprobación de límites.
- CVE-2014-4481 : Felipe Andres Manzano of the Binamuse VRT, via the iSIGHT Partners GVP Program

dyld

- Disponible para: iPhone 4s y posteriores, iPod touch (5ª generación) y posteriores, iPad 2 y posteriores.
- Impacto: un usuario local puede ser capaz de ejecutar código sin firmar
- Descripción: Existe un problema con la administración de estado en el manejo de archivos ejecutables Mach-O con segmentos superpuestos. Esta vulnerabilidad se resolvió mejorando

la validación de los tamaños de los segmentos.

- CVE-2014-4455 : TaiG Jailbreak Team

FontParser

- Disponible para: iPhone 4s y posteriores, iPod touch (5ª generación) y posteriores, iPad 2 y posteriores
- Impacto: La apertura de un archivo PDF malicioso especialmente diseñado puede provocar la finalización inesperada de aplicaciones o la ejecución de código arbitrario.
- Descripción: existe un desbordamiento de búfer en el manejo de los archivos de fuentes. Esta vulnerabilidad se resolvió mejorando la comprobación de límites.
- CVE-2014-4483: Apple

FontParser

- Disponible para: iPhone 4s y posteriores, iPod touch (5ª generación) y posteriores, iPad 2 y posteriores
- Impacto: El procesamiento de un archivo .dfont con fines malintencionados puede provocar la finalización inesperada de aplicaciones o la ejecución de código arbitrario.
- Descripción: Existe un problema de corrupción de memoria en el manejo de archivos .dfont. Esta vulnerabilidad se resolvió mejorando la comprobación de límites.
- CVE-2014-4484 : Gaurav Baruah working with HP's Zero Day Initiative

Foundation

- Disponible para: iPhone 4s y posteriores, iPod touch (5ª generación) y posteriores, iPad 2 y posteriores
- Impacto: la visualización de un archivo XML malicioso 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 resolvió mejorando la comprobación de límites.
- CVE-2014-4485: Apple

IOAcceleratorFamily

- Disponible para: iPhone 4s y posteriores, iPod touch (5ª generación) y posteriores, iPad 2 y posteriores
- Impacto: Una aplicación maliciosa puede ser capaz de ejecutar código arbitrario con privilegios de sistema.
- Descripción: Existe una referencia a un apuntador nulo en el manejo de listas de recursos de IOAcceleratorFamily. Esta vulnerabilidad se resolvió mediante la eliminación de código innecesario.
- CVE-2014-4486 : Ian Beer of Google Project Zero

IOHIDFamily

- Disponible para: iPhone 4s y posteriores, iPod touch (5ª generación) y posteriores, iPad 2 y posteriores
- 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 resolvió a través de la validación mejorada de tamaño.
- CVE-2014-4487 : TaiG Jailbreak Team

IOHIDFamily

- Disponible para: iPhone 4s y posteriores, iPod touch (5ª generación) y posteriores, iPad 2 y posteriores
- Impacto: Una aplicación maliciosa puede ser capaz de ejecutar código arbitrario con privilegios de sistema.
- Descripción: Existe un problema de validación en el manejo de metadatos de la cola de recursos de IOHIDFamily. Esta vulnerabilidad se resolvió mejorando la validación de los metadatos.
- CVE-2014-4488: Apple

IOHIDFamily

- Disponible para: iPhone 4s y posteriores, iPod touch (5ª generación) y posteriores, iPad 2 y posteriores
- Impacto: Una aplicación maliciosa puede ser capaz de ejecutar código arbitrario con privilegios de sistema.
- Descripción: Existe una referencia a un apuntador nulo en el manejo de colas de eventos de IOHIDFamily. Esta vulnerabilidad se resolvió mejorando la validación.
- CVE-2014-4489: @beist

iTunes Store

- Disponible para: iPhone 4s y posteriores, iPod touch (5ª generación) y posteriores, iPad 2 y posteriores
- Impacto: un sitio web puede ser capaz de eludir las restricciones de la sandbox utilizada por iTunes Store.
- Descripción: Existe un problema en el manejo de las redirecciones de Safari a la tienda iTunes Store que podrían permitir a un sitio web malicioso restricciones del entorno limitado de Safari. Esta vulnerabilidad se resolvió con un mejor filtrado de URLs abiertas por la tienda iTunes Store.
- CVE-2014-8840 : lokihardt@ASRT working with HP's Zero Day Initiative

Kernel

- Disponible para: iPhone 4s y posteriores, iPod touch (5ª generación) y posteriores, iPad 2 y posteriores
- Impacto: Aplicaciones de iOS maliciosas o comprometidas pueden ser capaces de determinar las direcciones del kernel.
- Descripción: un problema de divulgación de información existente en el manejo de las API relacionadas con las extensiones de kernel. Las respuestas que contienen una clave OSBundleMachOHeaders pueden haber incluido direcciones del kernel, que pueden ayudar a evadir la protección del espacio de direcciones aleatorias del diseño. Esta vulnerabilidad se resolvió quitando el desplazamiento de las direcciones antes de devolverlas.
- CVE-2014-4491:PanguTeam, Stefan Esser

Kernel

- Disponible para: iPhone 4s y posteriores, iPod touch (5ª generación) y posteriores, iPad 2 y posteriores
- Impacto: Una aplicación maliciosa puede ser capaz de ejecutar código arbitrario con privilegios de sistema.
- Descripción: Existe un problema en el kernel del subsistema de memoria compartida que permite a un atacante escribir en la memoria que estaba destinada a ser de sólo lectura. Esta vulnerabilidad se resolvió con la comprobación estricta de los permisos de memoria compartida.
- CVE-2014-4495 : Ian Beer of Google Project Zero

Kernel

- Disponible para: iPhone 4s y posteriores, iPod touch (5ª generación) y posteriores, iPad 2 y posteriores
- Impacto: Aplicaciones iOS maliciosas o comprometidas pueden ser capaces de determinar las direcciones del kernel.
- Descripción: La interfaz del kernel mach_port_kobject filtra direcciones del kernel y valores de permutación de almacenamiento dinámico, que puede ayudar a evadir la protección del espacio de direcciones aleatorias del diseño. Esta vulnerabilidad se resolvió mediante la desactivación de la interfaz mach_port_kobject en configuraciones de producción.
- CVE-2014-4496: Taig Jailbreak Equipo

ibnetcore

- Disponible para: iPhone 4s y posteriores, iPod touch (5ta generación) y posteriores, iPad 2 y posteriores.
- Impacto: Una app maliciosa o sandboxed app puede comprometer el demonio networkd.
- Descripción: Múltiples problemas de confusión de tipo existen en el manejo de networkd para la comunicación entre procesos. Mediante el envío de un mensaje con formato malicioso para networkd, puede ser posible ejecutar código arbitrario como el mismo proceso. El problema se resolvió mediante la comprobación adicional de tipos.
- CVE-2014-4492: Ian Beer de Google Project Zero

MobileInstallation

- Disponible para: iPhone 4s y posteriores, iPod touch (5ta generación) y posteriores, iPad 2 y posteriores.
- Impacto: Una aplicación empresarial maliciosa firmada puede ser capaz de tomar el control del contenedor local para las aplicaciones que están en un dispositivo.
- Descripción: Existe una vulnerabilidad en el proceso de instalación de la aplicación. Esto se abordó mediante la prevención de que las aplicaciones empresariales reemplacen a las aplicaciones existentes en escenarios específicos.
- CVE-2014-4493: Hui Xue y Tao Wei de FireEye, Inc.

Springboard

- Disponible para: iPhone 4s y posteriores, iPod touch (5ta generación) y posteriores, iPad 2 y posteriores.
- Impacto: Las aplicaciones empresariales con firma podrían ponerse en marcha sin pedir relación de confianza.
- Descripción: El problema consiste en determinar cuándo debe solicitarse la relación de confianza al abrir una aplicación empresarial firmada. Esta vulnerabilidad se soluciona mejorando la validación de la firma de código.
- CVE-2014-4494 : Song Jin, Hui Xue, y Tao Wei de FireEye, Inc.

WebKit

- Disponible para: iPhone 4s y posteriores, iPod touch (5ta generación) y posteriores, iPad 2 y posteriores.
- Impacto: La visita a un sitio web que enmarca el contenido malicioso puede llevar a la suplantación de la interfaz de usuario.
- Descripción: Un problema de suplantación de IU existía en el manejo de los límites de la barra de desplazamiento. Esta vulnerabilidad se resolvió mejorando la comprobación de límites.
- CVE-2014-4467 : Jordan Milne

WebKit

- Disponible para: iPhone 4s y posteriores, iPod touch (5ta generación) y posteriores, iPad 2 y posteriores.
- Descripción: Un SVG cargado en un elemento img podría incluir un archivo CSS de origen cruzado. Esta cuestión fue tratada mediante un bloqueo de las referencias CSS externas en IVS.
- Impacto: Las hojas de estilo que se cargan como origen cruzado pueden permitir la extracción de datos.
- CVE-2014-4465 : Rennie deGraaf of iSEC Partners

WebKit

- Disponible para: iPhone 4s y posteriores, iPod touch (5ta generación) y posteriores, iPad 2 y posteriores.
- Descripción: Varios problemas de corrupción de memoria existían en WebKit. Estas vulnerabilidades se resolvieron mejorando la gestión de memoria.
- Impacto: La visita a un sitio web malicioso puede provocar la finalización inesperada de una aplicación o la ejecución de código arbitrario.
- CVE-2014-3192 : cloudfuzzer
- CVE-2014-4459
- CVE-2014-4466 : Apple
- CVE-2014-4468 : Apple
- CVE-2014-4469 : Apple
- CVE-2014-4470 : Apple
- CVE-2014-4471 : Apple
- CVE-2014-4472 : Apple
- CVE-2014-4473 : Apple
- CVE-2014-4474 : Apple
- CVE-2014-4475 : Apple
- CVE-2014-4476 : Apple
- CVE-2014-4477 : lokihardt@ASRT trabaja con la iniciativa Día Cero de HP
- CVE-2014-4479 : Apple

2. Referencias

http://support.apple.com/en-us/HT204245

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

- Ricardo Andres Carmona Dominguez (rcarmona 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