Boletin de Seguridad UNAM-CERT-2015-008 iOS 8.2

Este documento describe el contenido de seguridad relacionado con iOS 8.2

- **Fecha de Liberación:** 10-Mar-2015
- **Ultima Revisión:** 12-Mar-2015
- **Fuente:**
- **CVE ID:** CVE-2015-1061 CVE-2015-1062 CVE-2015-1063 CVE-2015-1064 CVE-2015-1065 CVE-2015-1067

1. Descripción

CoreTelephony

- Disponible para: iPhone 4s y después, iPod touch (5th generation) y después, iPad 2 y después
- Un atacante de manera remota puede causar que un dispositivo reinicie de manera inesperada.
- Existía un puntero nulo que no referenciaba al momento de manejar los mensajes de Class 0 SMS en CoreTelephony. Esta vulnerabilidad se resolvió al mejorar la validación de mensajes.

IOSurface

- Disponible para: iPhone 4s y después, iPod touch (5th generation) y después, iPad 2 y después
- Impacto: Una aplicación maliciosa puede ejecutar código arbitrario con privilegios del sistema.
- Descripción: Existía una vulnerabilidad en el manejo de objetos seriados en IOSurface. Esta vulnerabilidad se resolvió agregando diversos tipos de verificación.

MobileStorageMounter

- Disponible para: iPhone 4s y después, iPod touch (5th generation) y después, iPad 2 y después
- Impacto: Una aplicación maliciosa puede crear carpetas en direcciones de confianza de archivos del sistema.
- Descripción: Existía una vulnerabilidad en el procedimiento al montar de manera lógica un disco resultando que carpetas inválidas no sean eliminadas de la imagen del disco. Esta vulnerabilidad fue resuelta al mejorar la gestión de errores.

Secure Transport

- Disponible para: iPhone 4s y después, iPod touch (5th generation) y después, iPad 2 y después
- Impacto: Un atacante con privilegios en la red puede interceptar conexiones SSL/TLS.
- Descripción: Descripción: Secure Transport acepta pequeñas llaves RSA, usualmente utilizadas solamente para exportar las suites de cifrado export-strength RSA, en conexiones que utilizan full-strength RSA. Esta característica, permite conocer como FREAK, sólo afecta conexiones al servidor que soportan las suites de cifrado export-strength RSA.

Springboard

- Disponible para: iPhone 4s y después, iPod touch (5th generation) y después, iPad 2 y después
- Impacto: Una persona que tenga acceso fisicamente a un dispositivo puede ver la pantalla principal incluso si el dispositivo se encuentra desactivado.
- Descripción: La terminación inesperada de una aplicación durante la activación podría causar que el dispositivo muestre la pantalla de inicio. Esta vulnerabilidad se resolvió mejorando el manejo de errores durante la activación.

2. Referencias

- https://support.apple.com/en-us/HT204423
- https://support.apple.com/en-us/ht1222

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