UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2005−013

Diversas vulnerabilidades afectan a productos Mac de Apple

Apple ha liberado la actualización de seguridad 2005−007 para corregir diversas vulnerabilidades que afectan a Mac OS X, Mac OS X Server, el navegador web Safari y otros productos. La más seria de estas vulnerabilidades podría permitir a un intruso remoto ejecutar código arbitrario. Los impactos de las otras vulnerabilidades incluyen esquivar restricciones de seguridad y negación de servicio.

Fecha de Liberación:	17 de Agosto de 2005
Ultima Revisión:	11 de Octubre de 2005
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión.

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Sistemas afectados

- Mac OS X de Apple, versiones 10.3.9 (Panther) y 10.4.2 (Tiger)
- Mac OS X Server de Apple, versiones 10.3.9 y 10.4.2
- Navegador web Safari de Apple

Ver Actualización de Seguridad de Apple 2005−007 para mayor información.

II. Descripción

La actualización de seguridad de Apple 2005−007 corrige varias vulnerabilidades que afectan al sistema operativo Mac OS X, OS X Server, el navegador Safari, y otros productos. Mas detalles se pueden encontrar en las siguientes notas de seguridad:

VU#913820 − Mac OS X de Apple contiene un buffer overflow en los servicios de directorios

Un buffer overflow en el proceso de autenticación del servicio de directorio en Mac OS X de Apple podría permitir a un atacante remoto no autentificado ejecutar código arbitrario en el sistema vulnerable. (CAN−2005−2507)

VU#461412 − Servermgrd de Mac OS X Server es vulnerable a un buffer overflow

Servermgrd de Mac OS X Server contiene una vulnerabilidad de tipo buffer overflow en las rutinas de autenticación. Esta vulnerabilidad podría permitir la ejecución remota de código arbitrario. (CAN−2005−2518)

VU#435188 − AppKit de Mac OS X vulnerable a un buffer overflow por medio de archivos enriquecidos de texto (.rtf) maliciosos.

Existe una vulnerabilidad de tipo buffer overflow en un componente del sistema operativo Mac OS X de Apple que maneja archivos .rtf. (CAN−2005−2501)

VU#172948 − AppKit de Mac OS X vulnerable a un buffer overflow por medio de archivos de Microsoft Word maliciosos.

Existe una vulnerabilidad de tipo buffer overflow en un componente del sistema operativo Mac OS X de Apple que maneja archivos de Microsoft Word. (CAN−2005−2502)

VU#420316 − El navegador Safari de Mac OS X de Apple vulnerable a la ejecución de comandos arbitrarios por medio de URLS en archivos PDF.

Los controles de seguridad de WebKit y Safari de Mac OS X podrían ser ignorados, permitiendo posiblemente la ejecución de comandos remotos. (CAN−2005−2522)

VU#709220 − El navegador Safari de Apple falla al realizar verificaciones de seguridad en ligas en texto enriquecido.

El navegador Safari de Apple falla al realizar verificaciones de seguridad en ligas en texto enriquecido, lo cual podría permitir a un atacante ejecutar comandos arbitrarios en el sistema vulnerable. (CAN−2005−2516)

Por favor note que la actualización de seguridad 2005−007 corrige vulnerabilidades adicionales no descritas arriba. Conforme mas información sea revelada, publicaremos notas de vulnerabilidad individuales.

III. Impacto

El impacto de estas vulnerabilidades varía. Para mas información sobre el impacto específico, por favor revise las notas de vulnerabilidad. Entre las consecuencias potenciales se incluye la ejecución de forma remota de código arbitrario o comandos, evadir las restricciones de seguridad, y denegación de servicio.

IV. Solución

Instale una actualización

Instale la actualización descrita en la actualización de seguridad 2005−007 de Apple. Además, esta actualización esta disponible por medio de Apple Update.

Apéndice A. Referencias

- US−CERT: Nota de vulnerabilidad VU#913820 − <http://www.kb.cert.org/vuls/id/913820>
- US−CERT: Nota de vulnerabilidad VU#461412 − <http://www.kb.cert.org/vuls/id/461412>
- US−CERT: Nota de vulnerabilidad VU#435188 − <http://www.kb.cert.org/vuls/id/435188>
- US−CERT: Nota de vulnerabilidad VU#172948 − <http://www.kb.cert.org/vuls/id/172948>
- US−CERT: Nota de vulnerabilidad VU#420316 − <http://www.kb.cert.org/vuls/id/420316>
- US−CERT: Nota de vulnerabilidad VU#709220 − <http://www.kb.cert.org/vuls/id/709220>
- Actualización de seguridad 2005−007 de Apple − <http://docs.info.apple.com/article.html?artnum=302163>
- Mac OS X: Actualizando su software − <http://docs.info.apple.com/article.html?artnum=106704>

El Departamento de Seguridad en Cómputo/UNAM−CERT agradece el apoyo en la traducción, elaboración y revisión de éste Documento a:

- Ruben Aquino Luna (raquino at seguridad dot unam dot mx)
- David Jiménez Domínguez (djimenez at correo dot seguridad dot unam dot mx)

UNAM−CERT
Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Cómputo
E−Mail: seguridad@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 43