UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−018

Productos Apple Mac afectados por múltiples vulnerabilidades

Apple ha liberado su Actualización de Seguridad 2006−003 para corregir múltiples vulnerabilidades que afectan Mac OS X, Mac OS X Server, el navegador Web Safari, Mail 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 violaciones de restricciones de seguridad y negación de servicio.

Fecha de Liberación:	12 de Mayo de 2006
Ultima Revisión:	12 de Mayo de 2006
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión.
CVE ID:	**CVE−2006−1457**

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Sistemas afectados

- Apple Mac OS X versión 10.3.9 (Panther) y versión 10.4.6 (Tiger)
- Apple Mac OS X Server versión 10.3.9 y versión 10.4.6
- Apple Safari web browser
- Apple Mail

Las versiones anteriores de Mac OS X podrían también ser afectadas. Consulte la Actualización de Seguridad de Apple 2006−003 para mayor información.

II. Descripción

La Actualización de Seguridad de Apple 2006−003 resuelve un número de vulnerabilidades que afectan Mac OS X, OS X Server, el navegador Web Safari, Mail y otros productos. Información más detallada puede encontrarse disponible en las Notas de Vulnerabilidad individuales.

III. Impacto

Los impactos de estas vulnerabilidades varían. Para mayor información sobre impactos específicos, consulte las Notas de Vulnerabilidad. Las consecuencias potenciales incluyen ejecución remota de comandos o código arbitrario, violaciones de restricciones de seguridad y negación de servicio.

IV. Solución

- **Instalar una actualización**

  Instalar la Actualización de Seguridad de Apple 2006−003. Estas y otras actualizaciones están disponibles a través de Apple Update.

- **Deshabilitar la opción "Open 'safe' files after downloading"**

  Para protección adicional, deshabilite la opción "Open 'safe' files after downloading", como se especifica en el documento "Asegurando tu Navegador Web" (en inglés).

V. Apéndice A. Referencias

- Asegurando tu Navegador Web − <http://www.us−cert.gov/reading_room/securing_browser/#Safari>
- Actualización de Seguridad de Apple 2006−003 − <http://docs.info.apple.com/article.html?artnum=303737>
- Mac OS X: Actualizando tu 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:

- Israel Becerril Sierra (ibecerril at seguridad dot unam dot mx)
- Jesús Ramón Jiménez Rojas (jrojas at 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