

UNAM-CERT**Departamento de Seguridad en Cómputo****DGSCA-UNAM**

Boletín de Seguridad UNAM-CERT-2006-037

Actualización de Apple para múltiples vulnerabilidades

El CERT/UNAM-CERT, a través de sus equipos de respuesta a incidentes de Seguridad en Cómputo, informan que Apple ha liberado la actualización de seguridad 2006-007 para corregir diversas vulnerabilidades que afectan a Mac OS X, Mac OS X Server. Vulnerabilidades en OpenSSL, gzip y otros productos también son solucionadas. La vulnerabilidad más grave podría permitir a un atacante remoto ejecutar código arbitrario. Los atacantes podrían también tomar ventaja de otras vulnerabilidades menos graves para evadir restricciones de seguridad o para causar una negación de servicio. Estas vulnerabilidades afectan tanto a equipos basados en procesadores Intel como en PowerPC de Apple.

Fecha de Liberación: 29 de Noviembre de 2006

Ultima Revisión: 30 de Noviembre de 2006

Fuente: CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como foros y listas de discusión.

Sistemas Afectados

Mac OS X	.	==10.3.x
Mac OS X	.	==10.4.x

Riesgo

Alto

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Ejecución Remota de Código

I. Descripción

La actualización de seguridad 2006-007 de Apple corrige diversas vulnerabilidades que afectan a Mac OS X, Mac OS X Server y a otros productos. Mayores detalles sobre estas vulnerabilidades pueden ser consultados en las notas respectivas.

Esta actualización de seguridad también corrige vulnerabilidades previas en PHP, Perl, OpenSSL y gzip, estos paquetes son instalados con Mac OS X. Las vulnerabilidades de OpenSSL están documentadas en diversas notas. También hay información disponible a través de la página de OpenSSL. La información sobre las vulnerabilidades de gzip están disponibles en diversas notas.

II. Impacto

El impacto de estas vulnerabilidades varía. Para detalles específicos consultar las notas respectivas. Algunas potenciales consecuencias incluyen ejecución de código arbitrario, evasión de restricciones de seguridad y negación de servicio.

III. Solución

Instalar actualizaciones.

Instalar la actualización de seguridad de Apple 2006-007. Ésta y otras actualizaciones están disponibles a través de Apple Update o Apple Downloads.

IV. Referencias

- ◆ Notas de Vulnerabilidad para la Actualización de Seguridad de Apple 2006-007 –

<http://www.kb.cert.org/vuls/byid?searchview-007>

- ◆ Notas de Vulnerabilidad para Alerta de Seguridad OpenSSL [28 de Septiembre 2006] –

http://www.kb.cert.org/vuls/byid?searchviewcadv_20060928

- ◆ Nota de Vulnerabilidad VU#845620 –

<http://www.kb.cert.org/vuls/id/845620>

- ◆ Nota de Vulnerabilidad VU#933712 –

<http://www.kb.cert.org/vuls/id/933712>

- ◆ Nota de Vulnerabilidad VU#381508 –

<http://www.kb.cert.org/vuls/id/381508>

- ◆ Nota de Vulnerabilidad VU#554780 –

<http://www.kb.cert.org/vuls/id/554780>

UNAM-CERT

- ◆ Nota de Vulnerabilidad VU#596848 –

<http://www.kb.cert.org/vuls/id/596848>

- ◆ Nota de Vulnerabilidad VU#773548 –

<http://www.kb.cert.org/vuls/id/773548>

- ◆ Sobre el contenido de seguridad de la Actualización de Seguridad 2006-007 –

<http://docs.info.apple.com/article.html?artnum=304829>

- ◆ Mac OS X: Actualizando tu software –

<http://docs.info.apple.com/article.html?artnum=106704>

- ◆ Descargas de Apple –

<http://www.apple.com/support/downloads/>

- ◆ OpenSSL: Vulnerabilidades en OpenSSL

<http://www.openssl.org/news/vulnerabilities.html>

- ◆ Asegurando Tu Navegador Web –

http://www.us-cert.gov/reading_room/securing_browser/#Safari

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)
- J. Inés Gervacio Gervacio (jgervacio at seguridad dot unam dot mx)
- Eduardo Espina (eespina 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