UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−008

Vulnerabilidad en Safari en Apple Mac OS X que permite la ejecución de comandos arbitrarios

---

El CERT/UNAM−CERT, a través de sus equipos de respuesta a incidentes de Seguridad en Cómputo, informan que existe una vulnerabilidad en Apple Safari determinada por cierto tipo de archivos permite que un intruso pueda ejecutar remotamente comandos arbitrarios en un sistema vulnerable

Fecha de Liberación:	22 de Febrero de 2006
Ultima Revisión:	22 de Febrero 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 **Safari** ==Todas

Riesgo

Moderado

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Ejecución Remota de Código

I. **Descripción**

Apple Safari es un navegador Web el cual viene con Mac OS X. La configuración por default de Safari permite de forma automática "Abrir archivos luego de ser descargados". Debido a la configuración por default de Safari y a la inconsistencia con la que Safari y OS X determinan la forma en la que guardan los archivos, es como Safari podrá ejecutar comandos arbitrarios

luego de visitar una página Web diseñada especialmente para el ataque.

Los detalles pueden verse en la siguiente Nota de Vulnerabilidad:
VU#999708 − Apple Safari permite la ejecución de comandos arbitrarios de forma automática.

II. Impacto

De forma remota, sin previa autenticación un intruso podrá ejecutar comandos arbitrarios con los privilegios del usuario que está ejecutando el navegador Safari. Si el administrador se autenticó de tal manera que cuenta con privilegios de administrador, el intruso podrá tomar control sin limitantes sobre el sistema vulnerable.

III. Solución

Desde el momento en el que no se conoce alguna actualización para solucionar este tipo de problema, se recomienda desactivar esta opción de forma manual.

Solución temporal

Desactivar "Abrir archivos seguros al descargarlos" que se encuentra en la pestaña "General" de las preferencias del navegador Safari.

IV. Apéndice A. Referencias

- US−CERT Vulnerability Note VU#999708 − http://www.kb.cert.org/vuls/id/999708
- Securing Your Web Browser − http://www.us−cert.gov/reading_room/securing_browser/#sgeneral
- Apple − Mac OS X − Safari RSS − http://www.us−cert.gov/reading_room/securing_browser/#sgeneral

---

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)
- Ruben Aquino Luna (raquino 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