

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

Boletín de Seguridad UNAM-CERT-2008-011

Actualizaciones de Mozilla para múltiples vulnerabilidades.

Nuevas versiones de Firefox, Thunderbird y SeaMonkey corrigen múltiples vulnerabilidades, la más severa de éstas podría permitir a un atacante ejecutar código arbitrario de manera remota en un sistema afectado.

Fecha de Liberación: 28 de Marzo de 2008

Última Revisión: 31 de Marzo de 2008

Fuente: CERT/CC

Sistemas Afectados

Mozilla	=Firefox
Mozilla	=SeaMonkey
Mozilla	=Thunderbird

Riesgo

Alto

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Descripción

Los proyectos Mozilla y SeaMonkey han liberado las nuevas versiones de Firefox, Thunderbird y SeaMonkey para corregir varias vulnerabilidades. Más detalles acerca de estas vulnerabilidades están disponibles en Mozilla Foundation Security Advisories y en la Base de Datos de Vulnerabilidades del CERT/CC. Un atacante puede explotar estas vulnerabilidades convenciendo a un usuario de que vea un documento HTML manipulado especialmente, como una página web o un mensaje de correo electrónico HTML.

II. Impacto

Mientras los impactos de las vulnerabilidades individuales varía, el más severo puede permitir que usuarios sin autorización puedan ejecutar código arbitrario de manera remota en un sistema vulnerable. Un atacante también puede provocar una denegación de servicio o ejecutar ataques de cross-site scripting.

III. Solución

Actualizar

Estas vulnerabilidades están corregidas en Mozilla Firefox 2.0.0.13, Thunderbird 2.0.0.13, y SeaMonkey 1.1.9.

Desactivar JavaScript

Algunas de estas vulnerabilidades pueden mitigarse deshabilitando JavaScript o utilizando la extensión NoScript. Para obtener más información acerca de la configuración de Firefox, por favor vea el documento [Securing Your Web Browser](#). Thunderbird deshabilita JavaScript por omisión.

IV. Referencias

- ◆ US-CERT Vulnerability Notes – <http://www.kb.cert.org/vuls/byid?searchview0803>
- ◆ Securing Your Web Browser – http://www.us-cert.gov/reading_room/securing_browser/browser_security.html#Mozilla_Firefox
- ◆ Mozilla Foundation Security Advisories – <http://www.mozilla.org/security/announce>
- ◆ Known Vulnerabilities in Mozilla Products – <http://www.mozilla.org/projects/security/known-vulnerabilities.html>
- ◆ Mozilla Hall of Fame – <http://www.mozilla.org/university/HOF.html>

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)
- José Roberto Sánchez Soledad (rsanchez at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Cómputo
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