UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−025

Los productos Mozilla contienen múltiples vulnerabilidades

El CERT/UNAM−CERT, a través de sus equipos de respuesta a incidentes de Seguridad en Cómputo, informan que el navegador web Mozilla y productos derivados contienen diversas vulnerabilidades, la más seria podría permitir a un atacante remoto ejecutar código arbitrario en el sistema afectado.

Fecha de Liberación:	27 de Julio de 2006
Ultima Revisión:	28 de Julio de 2006
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión.

Sistemas Afectados

Mozilla Firefox	<1.5.0.5
Mozilla SeaMonkey	<1.0.3
Mozilla Thunderbird	<1.5.0.5

Riesgo

Importante

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. **Descripción**

Varias vulnerabilidades han sido reportadas en el navegador web Mozilla y productos derivados. Información detallada esta disponible en cada una de las notas de vulnerabilidades, incluyendo las siguientes:

VU#476724 − Productos Mozilla fallan en el manejo apropiado de referencias a frames

Los productos Mozilla fallan al manejar apropiadamente las referencias a frames o ventanas. Esto podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable. (CVE−2006−3801)

VU#670060 − Mozilla falla al liberar referencias de JavaScript.

Los productos Mozilla fallan al liberar memoria de forma apropiada. Esta vulnerabilidad podría permitir a un intruso remoto ejecutar código en un sistema vulnerable. (CVE−2006−3677)

VU#239124 − Mozilla falla al manejar eventos XPCOM simultáneos de forma apropiada.

Los productos Mozilla son vulnerables a una corrupción en memoria por medio de eventos XPCOM simultáneos. Esto podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable. (CVE−2006−3113)

VU#265964 − Los productos Mozilla contienen un race condition

Los productos Mozilla contienen un race condition. Esta vulnerabilidad podría permitir a un intruso remoto ejecutar código en un sistema vulnerable. (CVE−2006−3803)

VU#897540 − Los productos Mozilla son afectados por un buffer overflow en datos VCard adjuntos

Los productos Mozilla fallan en el manejo apropiado de datos adjuntos mal formados de tipo VCard, permitiendo que ocurra un buffer overflow. Esta vulnerabilidad podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable. (CVE−2006−3804)

II. Impacto

Un intruso remoto, no autenticado podría ejecutar código arbitrario en un sistema vulnerable. Un intruso también podría provocar que una aplicación vulnerable deje de funcionar.

III. Solución

Actualizar

Actualizar a Mozilla Firefox 1.5.0.5, Mozilla Thunderbird 1.5.0.5, o SeaMonkey 1.0.3.

Deshabilitar JavaScript y Java

Estas vulnerabilidades pueden mitigarse deshabilitando Javascript y Java en todos los productos afectados. Las instrucciones para deshabilitar Java en Firefox pueden encontrarse en el documento "Asegurando tu navegador web".

IV. Apéndice A. Referencias

- Notas de vulnerabilidad relacionadas con los boletines de seguridad de Mozilla de julio − <http://www.kb.cert.org/vuls/byid?searchview05>
- CVE−2006−3081 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−3801>
- CVE−2006−3677 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−3677>
- CVE−2006−3113 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−3113>
- CVE−2006−3803 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−3803>
- CVE−2006−3804 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−3804>
- CVE−2006−3805 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−3805>
- CVE−2006−3806 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−3806>
- CVE−2006−3807 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−3807>
- CVE−2006−3811 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−3811>
- Boletines de seguridad de la Fundación Mozilla − <http://www.mozilla.org/security/announce/>
- Vulnerabilidades conocidas en los productos Mozilla − <http://www.mozilla.org/projects/security/known−vulnerabilities.html>
- Asegurando tu navegador web − <http://www.us−cert.gov/reading_room/securing_browser/browser_security.html#Mozilla_Firefox>

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