UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−035

Actualizaciones de Mozilla para Múltiples Vulnerabilidades

El navegador Web Mozilla y sus productos derivados contienen varias vulnerabilidades, la más seria de ellas podría permitir a un intruso remoto ejecutar código arbitrario en un sistema afectado.

Fecha de Liberación:	8 de Noviembre de 2006
Ultima Revisión:	8 de Noviembre de 2006
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como foros y listas de discusión.

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Ejecución Remota de Código

I. **Sistemas afectados**

- Mozilla SeaMonkey
- Mozilla Firefox
- Mozilla Thunderbird
- Netscape web browser

II. **Descripción**

Varias vulnerabilidades han sido reportadas en el navegador de Web Mozilla y sus productos derivados. Mozilla ha vuelto a liberar tres avisos de seguridad para describir las vulnerabilidades.

Mozilla Foundation Security Advisory 2006−67 está relacionado con una vulnerabilidad de ejecución remota de código en la forma en como JavaScript es

manejado por Firefox, Thunderbird, y SeaMonkey. Más información puede ser encontrada en la Nota de Vulnerabilidad VU#714496.

Mozilla Foundation Security Advisory 2006−66 está relacionado con una vulnerabilidad en la forma en como las firmas RSA son manejadas por Firefox, Thunderbird, y SeaMonkey. Más información puede ser encontrada en la Nota de Vulnerabilidad VU#335392.

Mozilla Foundation Security Advisory 2006−65 está relacionado con tres vulnerabilidades de corrupción de memoria en Firefox, Thunderbird y SeaMonkey. Más información puede ser encontrada en la Notas de Vulnerabilidades VU#815432, VU#390480, y VU#495288.

Cualquier producto basado en componentes de Mozilla, especialmente Gecko, podría ser afectado por las vulnerabilidades cubiertas en VU#714496, VU#815432, VU#390480, y VU#495288.

Cualquier software que utilice Mozilla NSS (Network Security Services) podría ser afectado por la vulnerabilidad cubierta en VU#335392.

III. Impacto

El impacto más severo de estas vulnerabilidades podría permitir a un intruso remoto ejecutar código arbitrario con los privilegios del usuario ejecutando la aplicación afectada. Otros efectos incluyen la falsificación de firmas RSA y negación de servicio. Un intruso remoto no autenticado podría ejecutar código arbitrario o causar una negación de servicio.

La falsificación de una firma RSA (VU#335392) podría permitir a un intruso crear un certificado TLS/SSL o de correo electrónico que no será detectado como inválido. Esto podría permitir que un intruso personifique un sitio Web o un sistema de correo electrónico que confíe en certificados para realizar autenticación.

IV. Solución

- **Actualice su software.**

  Estas vulnerabilidades están solucionadas en Firefox 1.5.0.8, Mozilla Thunderbird 1.5.0.8, y SeaMonkey 1.0.6.

  De acuerdo a Mozilla:

  > Firefox 1.5.0.x será mantenido con actualizaciones de seguridad y estabilidad hasta el 24 de abril de 2007. Se recomienda a todos los usuarios actualizar a Firefox 2.

V. Apéndice

- Nota de Vulnerabilidad VU#714496 − <http://www.kb.cert.org/vuls/id/714496>
- Nota de Vulnerabilidad VU#335392 − <http://www.kb.cert.org/vuls/id/335392>
- Nota de Vulnerabilidad VU#815432 − <http://www.kb.cert.org/vuls/id/815432>
- Nota de Vulnerabilidad VU#390480 − <http://www.kb.cert.org/vuls/id/390480>
- Nota de Vulnerabilidad VU#495288 − <http://www.kb.cert.org/vuls/id/495288>
- Avisos de Seguridad de Mozilla Foundation −

<http://www.mozilla.org/security/announce/>
- Vulnerabilidades Conocidas en Productos de Mozilla − <http://www.mozilla.org/projects/security/known−vulnerabilities.html>
- Asegura tu Navegador Web (inglés) − <http://www.us−cert.gov/reading_room/securing_browser/browser_security.html#Mozilla_Firefox>
- Mozilla Hall of Fame − <http://www.mozilla.org/university/HOF.html>
- Controles de Sitios (en inglés) − <http://browser.netscape.com/ns8/help/options−site.jsp>

El Departamento de Seguridad en Cómputo/UNAM−CERT agradece el apoyo en la traducción, elaboración y revisión de éste Documento a:

- 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