UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−014

Múltiples vulnerabilidades en productos Mozilla

Varias vulnerabilidades han sido reportadas en el navegador web Mozilla y productos derivados, la más seria podría permitir a un atacante remoto ejecutar código arbitrario en un sistema afectado.

Fecha de Liberación: 17 de Abril de 2006

Ultima Revisión: 20 de Abril de 2006

Fuente: http://www.us−cert.gov/cas/techalerts/TA06−107A.html

Riesgo

Alto

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Ejecución remota de código y negación de servicio

I. **Descripción**

Varias vulnerabilidades han sido reportadas en el navegador web Mozilla y productos derivados. Información mas detallada está disponible en las notas de vulnerabilidad individuales, incluyendo:

VU#932734 − Vulnerabilidad en crypto.generateCRMFRquest() de Mozilla

Existe una vulnerabilidad en la rutina JavaScript generateCRMFRquest() de Mozilla que podría permitir a un atacante remoto ejecutar código arbitrario. (CVE−2006−1728)

VU#968814 − Vulnerabilidad en seguridad JavaScript de Mozilla

Los productos Mozilla fallan en el manejo de las restricciones de seguridad en JavaScript. Esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario. (CVE−2006−1726)

VU#179014 − Vulnerabilidad integer overflow en CSS de Mozilla

Los productos Mozilla contienen una vulnerabilidad de tipo integer overflow que podría permitir a un atacante remoto no autenticado ejecutar código arbitrario. (CVE−2006−1730)

VU#488774 − Vulnerabilidad en XBL de Mozilla

Los productos Mozilla fallan al restringir el acceso a código XBL privilegiado. Esta vulnerabilidad podría permitir a un atacante remoto no autenticado ejecutar código arbitrario. (CVE−2006−1733)

VU#842094 − Vulnerabilidad en función JavaScript "clone parent" en Mozilla

Los productos Mozilla fallan al restringir el acceso a las funciones JavaScript "clone parent". Esta vulnerabilidad podría permitir a un atacante ejecutar código arbitrario en un sistema vulnerable. (CVE−2006−1734)

VU#813230 − Productos Mozilla vulnerables a escalación de privilegios mediante XBL.method.eval

Una vulnerabilidad en la manera en que los productos Mozilla y programas derivados manejan ciertos métodos XBL podría permitir a un atacante remoto ejecutar código arbitrario en un sistema vulnerable. (CVE−2006−1735)

VU#736934 − Productos Mozilla vulnerables a corrupción de memoria mediante una secuencia de etiquetas HTML en particular

Una vulnerabilidad en la manera en que los productos Mozilla y programas derivados manejan ciertas etiquetas HTML podría permitir a un atacante remoto ejecutar código arbitrario en un sistema vulnerable. (CVE−2006−0749)

VU#935556 − Productos Mozilla podrían permitir que código CSS escribir mas allá del final de un arreglo

Una vulnerabilidad en la manera en que productos Mozilla y programas derivados manejan ciertos métodos CSS podría permitir a un atacante remoto terminar la aplicación o ejecutar código arbitrario en un sistema vulnerable. (CVE−2006−1739)

VU#350262 − Vulnerabilidades de corrupción de memoria por DHTML en Mozilla

Los productos Mozilla contienen varias vulnerabilidades no especificadas en la manera en como manejan el DHTML. Estas vulnerabilidades podrían permitir a un atacante remoto ejecutar código arbitrario o causar una negación de servicio. (CVE−2006−1724)

VU#252324 − Vulnerabilidad en el despliegue de estilos en Mozilla

Los productos Mozilla contienen una vulnerabilidad no especificada en la forma en que manejan el despliegue de estilos. Esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario o causar una negación de servicio.

VU#329500 − Productos Mozilla vulnerables a una corrupción en memoria debido a una expresión regular larga en JavaScript

Una vulnerabilidad en la manera en que el motor JavaScript de los productos Mozilla y programas derivados manejan una expresión regular larga y podría permitir que un atacante remoto termine la aplicación o ejecute código arbitrario en un sistema vulnerable.

II. Impacto

El impacto mas severo de estas vulnerabilidades podría permitir a un atacante remoto la ejecución de código con los privilegios del usuario que ejecute la aplicación. Otros efectos incluyen una negación de servicio o acceso a la información local.

III. Solución

Actualizar a Mozilla Firefox 1.5.0.2, Mozilla Thunderbird 1.5.0.2 ó SeaMonkey 1.0.1. De acuerdo con Mozilla.org, Thunderbird 1.5.0.2 será liberado el 18 de Abril del 2006.

Se recomienda a los usuarios aplicar las opciones descritas en la nota individual de la vulnerabilidad antes de que las actualizaciones sean aplicadas.

IV. Apéndice A. Referencias

- Avisos de Seguridad de la Fundación Mozilla − http://www.mozilla.org/security/announce/
- Avisos de Seguridad de la Fundación Mozilla − http://www.mozilla.org/projects/security/known−vulnerabilities.html
- Nota de vulnerabilidad US−CERT VU#932734 − http://www.kb.cert.org/vuls/id/932734
- Nota de vulnerabilidad US−CERT VU#968814 − http://www.kb.cert.org/vuls/id/968814
- Nota de vulnerabilidad US−CERT VU#179014 − http://www.kb.cert.org/vuls/id/179014
- Nota de vulnerabilidad US−CERT VU#488774 − http://www.kb.cert.org/vuls/id/488774
- Nota de vulnerabilidad US−CERT VU#842094 − href=http://www.kb.cert.org/vuls/id/842094
- Nota de vulnerabilidad US−CERT VU#813230 − href=http://www.kb.cert.org/vuls/id/813230
- Nota de vulnerabilidad US−CERT VU#736934 − href=http://www.kb.cert.org/vuls/id/736934
- Nota de vulnerabilidad US−CERT VU#935556 − href=http://www.kb.cert.org/vuls/id/935556
- Nota de vulnerabilidad US−CERT VU#350262 −

href=http://www.kb.cert.org/vuls/id/350262
- Nota de vulnerabilidad US−CERT VU#252324 − href=http://www.kb.cert.org/vuls/id/252324
- Nota de vulnerabilidad US−CERT VU#329500 − http://www.kb.cert.org/vuls/id/329500
- Nota de vulnerabilidad US−CERT Relacionada con el Aviso de Seguridad de Mozilla en Abril − http://www.kb.cert.org/vuls/byid?searchviewril_2006
- CVE−2006−1726 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1726
- CVE−2006−1728 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1728
- CVE−2006−1730 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1730
- CVE−2006−1733 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1733
- CVE−2006−1734 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1734
- CVE−2006−1735 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1735
- CVE−2006−0749 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0749
- CVE−2006−1739 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1739
- CVE−2006−1724 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1724
- Firefox − Redescubre el Web− http://www.mozilla.com/firefox/
- Thunderbird − Reclama tu correo − http://www.mozilla.com/thunderbird
- El Proyecto SeaMonkey − http://www.mozilla.org/projects/seamonkey/
- Mozilla Suite − Suite de Aplicación de Internet todo en uno − http://www.mozilla.org/products/mozilla1.x/
- 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:

- Sergio Alavez Miguel (salavez at seguridad dot unam dot mx)
- J. Inés Gervacio Gervacio (jgervacio 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