

UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA-UNAM

Boletín de Seguridad UNAM-CERT-2006-006

Múltiples Vulnerabilidades en Productos Mozilla

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

Fecha de Liberación: 7 de Febrero de 2006

Ultima Revisión: 8 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

Firefox web browser
Mozilla mail client
Mozilla web browser
Thunderbird mail client

Riesgo

Alto

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 está disponible en las notas individuales de las vulnerabilidades:

* VU#592425 – Productos basados en mozilla fallan al validar la entrada del usuario en el atributo del nombre en "XULDocument.persist"

Una vulnerabilidad en algunos productos Mozilla podrían permitir a un atacante remoto ejecutar comandos de Javascript con los permisos del usuario que está ejecutando la aplicación afectada.

* VU#759273 – Vulnerabilidad de corrupción de memoria en Mozilla QueryInterface

El navegador web Mozilla Firefox y el cliente de correo Thunderbird contienen una vulnerabilidad de corrupción de memoria que podría permitir a un atacante remoto ejecutar código arbitrario.

II. Solución

Actualizar a Mozilla Firefox 1.5.0.1 o SeaMonkey 1.0.

Para los productos basados en Mozilla que no tengan actualizaciones disponibles, se recomienda fuertemente a los usuarios deshabilitar JavaScript.

III. Impacto

El impacto más grave de estas vulnerabilidades es poder permitir a un atacante remoto ejecutar código arbitrario con los privilegios del usuario que está ejecutando la aplicación afectada. Otros daños incluyen una negación de servicio o acceso a la información local.

IV. Apéndice. Referencias

- ◆ Mozilla Foundation Security Advisories – [<http://www.mozilla.org/security/announce/>](http://www.mozilla.org/security/announce/)
- ◆ Mozilla Foundation Security Advisories – [<http://www.mozilla.org/projects/security/known-vulnerabilities.html>](http://www.mozilla.org/projects/security/known-vulnerabilities.html)
- ◆ US-CERT Vulnerability Note VU#592425 – [<http://www.kb.cert.org/vuls/id/592425>](http://www.kb.cert.org/vuls/id/592425)
- ◆ US-CERT Vulnerability Note VU#759273 – [<http://www.kb.cert.org/vuls/id/759273>](http://www.kb.cert.org/vuls/id/759273)
- ◆ US-CERT Vulnerability Notes Related to February Mozilla Security Advisories – [<http://www.kb.cert.org/vuls/byid?searchviewb_2006>](http://www.kb.cert.org/vuls/byid?searchviewb_2006)
- ◆ CVE-2006-0296 – [<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0296>](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0296)
- ◆ CVE-2006-0295 – [<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0295>](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0295)
- ◆ Firefox – Rediscover the Web – [<http://www.mozilla.com/firefox/>](http://www.mozilla.com/firefox/)
- ◆ The SeaMonkey Project – [<http://www.mozilla.org/projects/seamoney/>](http://www.mozilla.org/projects/seamoney/)

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)
-

UNAM-CERT

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