UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−014

Vulnerabilidades en Windows e Internet Explorer de Microsoft

El CERT/UNAM−CERT, a través de sus equipos de respuesta a incidentes de Seguridad en Cómputo, informan que Microsoft ha liberado actualizaciones que corrigen vulnerabilidades críticas en Windows e Internet Explorer. La explotación de estas vulnerabilidades podría permitir a un intruso remoto, no autenticado, ejecutar código arbitrario o provocar una negación de servicio en un sistema vulnerable.

Fecha de Liberación:	12 de Abril de 2006
Ultima Revisión:	12 de Abril de 2006
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión.

Sistemas Afectados

Microsoft Windows todas las versiones	**Internet Explorer**	== Todas
Microsoft Windows todas las versiones	**Windows**	== Todas

Riesgo

Crítico

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. **Descripción**

El resumen del Boletín de Seguridad de Microsoft para Abril de 2006 cubre vulnerabilidades en Windows e Internet Explorer de Microsoft. Se puede encontrar más información en las siguientes Notas de Vulnerabilidad del US−CERT:

VU#876678 − Vulnerabilidad en createTextRange() de Microsoft Internet Explorer

Internet Explorer, de Microsoft, no maneja adecuadamente el método createTextRange() DHTML, posiblemente permitiendo a un intruso remoto, no autenticado, ejecutar código arbitrario. (CVE−2006−1359)

VU#984473 − Internet Explorer de Microsoft contiene un desbordamiento al procesar manejadores script action.

Una vulnerabilidad en el navegador web Internet Explorer de Microsoft podría permitir a un intruso remoto detener la ejecución del navegador o podiblemente ejecutar código arbitrario en un sistema vulnerable. (CVE−2006−1245)

VU#434641 − Internet Explorer de Microsoft podría ejecutar automáticamente archivos HTA.

Internet Explorer de Microsoft no maneja adecuadamente los archivos HTA. Esta vulnerabilidad podría permitir a un intruso remoto ejecutar código arbitrario. (CVE−2006−1388)

VU#503124 − Internet Explorer de Microsoft no puede manejar HTML creado específicamente de forma maliciosa y malformado.

Internet Explorer de Microsoft no maneja adecuadamente HTML malformado. Esta vulnerabilidad podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable. (CVE−2006−1185)

VU#959049 − Multiples objetos COM provocan corrupción de memoria en Internet Explorer de Microsoft.

Internet Explorer de Microsoft permite instanciar objetos COM que no están designados para uso en el navegador, lo cual podría permitir a un intruso remoto ejecutar código arbitrario o detener la ejecución de IE. (CVE−2006−1186)

VU#824324 − Internet Explorer de Microsoft no maneja adecuadamente elementos HTML con un tag creado maliciosamente.

Internet Explorer de Microsoft no maneja adecuadamente etiquetas de elementos HTML, lo que podría permitir a un intruso remoto, no autenticado, ejecutar código arbitrario. (CVE−2006−1188)

VU#341028 − Internet Explorer de Microsoft no maneja adecuadamente caracteres de doble−byte en URLs creadas maliciosamente.

Internet Explorer de Microsoft no maneja adecuadamente caracteres de doble−byte en URLs, lo que podría permitir a un intruso remoto, no autenticado ejecutar código arbitrario. (CVE−2006−1189)

VU#234812 − Microsoft Windows contiene una vulnerabilidad en el control ActiveX RDS.Dataspace en MDAC

Microsoft Windows no maneja adecuadamente el control ActiveX RDS.Dataspace permitiendo, posiblemente, a un intruso remoto ejecutar código arbitrario. (CVE−2006−0003)

VU#641460 − Microsoft Windows Explorer no maneja adecuadamente los objetos COM

Microsoft Windows no maneja adecuadamente los objetos COM. Esta vulnerabilidad podría permitir a un intruso remoto, no autenticado, ejecutar código arbitrario en un sistema vulnerable. (CVE−2006−0012)

II. Impacto

Un intruso remoto puede ejecutar código malicioso con los privilegios del usuario que haya iniciado sesión. Si el usuario ha iniciado sesión con los privilegios del administrador del equipo, el intruso puede tomar control total del sistema. Además, el intruso puede ser capaz también de causar una negación de servicios.

III. Solución

Aplicar la actualización correspondiente.

Microsoft ha liberado la actualizaciones para estas vulnerabilidades en el sitio de Microsoft Update.

Soluciones Temporales

Por favor vea las soluciones temporales en las notas de vulnerabilidades del CERT. Algunas de estas vulnerabilidades listadas en este boletín pueden ser mitigadas con las instrucciones listadas en el documento Securing Your Web Browser del apéndice.

IV. Apéndice A. Referencias

- Microsoft Security Bulletin Summary for April 2006 − http://www.microsoft.com/technet/security/bulletin/ms06−apr.mspx
- US−CERT Vulnerability Note VU#876678 − http://www.kb.cert.org/vuls/id/876678
- US−CERT Vulnerability Note VU#984473 − http://www.kb.cert.org/vuls/id/984473
- US−CERT Vulnerability Note VU#434641 − http://www.kb.cert.org/vuls/id/434641
- US−CERT Vulnerability Note VU#503124 − http://www.kb.cert.org/vuls/id/503124
- US−CERT Vulnerability Note VU#959049 − http://www.kb.cert.org/vuls/id/959049
- US−CERT Vulnerability Note VU#824324 − http://www.kb.cert.org/vuls/id/824324
- US−CERT Vulnerability Note VU#341028 − http://www.kb.cert.org/vuls/id/341028

- US−CERT Vulnerability Note VU#234812 − http://www.kb.cert.org/vuls/id/234812
- US−CERT Vulnerability Note VU#641460 − http://www.kb.cert.org/vuls/id/641460
- CVE−2006−1359 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1359
- CVE−2006−1245 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1245
- CVE−2006−1388 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1388
- CVE−2006−1185 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1185
- CVE−2006−1186 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1186
- CVE−2006−1188 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1188
- CVE−2006−1189 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1189
- CVE−2006−0003 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0003
- CVE−2006−0012 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0012
- Microsoft Update − https://update.microsoft.com/microsoftupdate
- Securing Your Web Browser − http://www.us−cert.gov/reading_room/securing_browser/#Internet_Explorer

---

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)
- Luis Fernando Fuentes Serrano (lfuentes 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