UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−023

Vulnerabilidades en Microsoft Windows, Office, e IIS

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades críticas en Microsoft Windows, IIS, y Office. La explotación de éstas vulnerabilidades podría permitir a un intruso remoto no auntenticado ejecutar código arbitrario o causar una negación de servicio en un sistema vulnerable.

Fecha de Liberación:	11 de Julio de 2006
Ultima Revisión:	12 de Julio 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

Local y remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Sistemas afectados

- Microsoft Windows
- Microsoft Internet Information Services (IIS)
- Microsoft Office
- Microsoft Office para Mac
- Microsoft Access
- Microsoft Excel y Excel Viewer
- Microsoft FrontPage
- Microsoft InfoPath
- Microsoft OneNote
- Microsoft Outlook

- Microsoft PowerPoint
- Microsoft Project
- Microsoft Publisher
- Microsoft Visio
- Microsoft Word y Word Viewer

II. Descripción

El Resumen de Boletines de Seguridad de Microsoft para Julio de 2006 de 2006 soluciona vulnerabilidades en productos Microsoft incluyendo Windows, IIS y Office. Información adicional está disponible en las siguientes Notas de Vulnerabilidades del US−CERT.

- **VU#395588 − Microsoft Internet Information Services vulnerable a ejecución remota de código a través de archivo ASP creado de forma maliciosa**

  Microsoft Internet Information Services (IIS) contiene una vulnerabilidad de buffer overflow. Esta podría permitir a un intruso remoto no autenticado ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−0026)

- **VU#189140 − Microsoft Server Service Mailslot vulnerable a overflow de heap**

  Una vulnerabilidad de buffer overflow en el servicio de servidor de Microsoft Mailslot podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−1314)

- **VU#257164 − El servicio Cliente de DHCP de Microsoft contiene un buffer overflow**

  Una vulnerabilidad de buffer overflow en el servicio de servidor de Microsoft Mailslot podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−2372)

- **VU#802324 − Vulnerabilidad en Microsoft Excel**

  Una vulnerabilidad no especificada en Microsoft Excel podría permitir a un intruso ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−3059)

- **VU#580036 − Microsoft Office falla al manejar adecuadamente cadenas malformadas**

  Microsoft Office falla al manejar adecuadamente cadenas creadas de forma maliciosa. Esta vulnerabilidad podría permitir a un intruso remoto ejecutar código arbitrario.
  (CVE−2006−1316)

- **VU#609868 − Vulnerabilidad en análisis de cadenas en Microsoft Office**

  Microsoft Office falla al analizar adecuadamente cadenas. Esta vulnerabilidad podría permitir a un intruso remoto no autenticado ejecutar código arbitrario.
  (CVE−2006−1316)

- **VU#409316 − Microsoft Office falla al manejar adecuadamente propiedades de documentos**

  Microsoft Office contiene un buffer overflow cuando maneja propiedades de documentos creadas de forma maliciosa.
  (CVE−2006−2389)

- **VU#459388 − Microsoft Office falla al manejar adecuadamente imágenes PNG**

  Aplicaciones de Microsoft Office fallan al manejar adecuadamente imágenes PNG. Esta vulnerabilidad podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−0033)

- **VU#668564 − Microsoft Office falla al manejar adecuadamente imágenes GIF**

  Aplicaciones de Microsoft Office fallan al manejar adecuadamente imágenes GIF. Esta vulnerabilidad podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−0007)

III. Impacto

Un intruso remoto no autenticado podría ejecutar código arbitrario en un sistema vulnerable. Un intruso podría también ser capaz de causar una negación de servicio.

IV. Solución

- **Aplicar una actualización de su distribuidor.**

  Microsoft ha proporcionado actualizaciones para estas vulnerabilidades en sus Boletines de Seguridad. Actualizaciones para Microsoft Windows y Microsoft Office XP y versiones posteriores están disponibles en el sitio de Microsoft Update. Actualizaciones para Microsoft Office 2000 están disponibles en el sitio de Microsoft Office Update. Los usuarios de Mac OS X de Apple deberían obtener actualizaciones desde el sitio Web de Mactopia.

- **Soluciones temporales.**

  Consulte las siguientes Notas de Vulnerabilidades para obtener soluciones temporales.

Apéndice A. Referencias

- Proyecto Seguridad en Windows, DSC/UNAM−CERT − <http://www.seguridad.unam.mx/windows>
- Resumen de Boletines de Seguridad de Microsoft para Julio de 2006 − <http://www.microsoft.com/technet/security/bulletin/ms06−jul.mspx>
- Alerta de Seguridad Cibernética TA06−167A − <http://www.us−cert.gov/cas/techalerts/TA06−167A.html>
- Notas de Vulnerabilidad del US−CERT para actualizaciones de Julio de 2006 de Microsoft − <http://www.kb.cert.org/vuls/byid?searchview&query=ms06−jul>
- Nota de Vulnerabilidad del US−CERT VU#395588 − <http://www.kb.cert.org/vuls/id/395588>
- Nota de Vulnerabilidad del US−CERT VU#189140 − <http://www.kb.cert.org/vuls/id/189140>
- Nota de Vulnerabilidad del US−CERT VU#257164 − <http://www.kb.cert.org/vuls/id/257164>
- Nota de Vulnerabilidad del US−CERT VU#802324 − <http://www.kb.cert.org/vuls/id/802324>
- Nota de Vulnerabilidad del US−CERT VU#580036 − <http://www.kb.cert.org/vuls/id/580036>
- Nota de Vulnerabilidad del US−CERT VU#609868 − <http://www.kb.cert.org/vuls/id/609868>
- Nota de Vulnerabilidad del US−CERT VU#409316 − <http://www.kb.cert.org/vuls/id/409316>
- Nota de Vulnerabilidad del US−CERT VU#459388 − <http://www.kb.cert.org/vuls/id/459388>
- Nota de Vulnerabilidad del US−CERT VU#668564 − <http://www.kb.cert.org/vuls/id/668564>
- CVE−2006−0026 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0026>
- CVE−2006−1314 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1314>
- CVE−2006−2372 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−2372>
- CVE−2006−3059 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−3059>
- CVE−2006−1316 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1316>
- CVE−2006−1540 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1540>
- CVE−2006−2389 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−2389>
- CVE−2006−0033 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0033>
- CVE−2006−0007 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0007>
- Microsoft Update − <https://update.microsoft.com/microsoftupdate>
- Microsoft Office Update − <http://officeupdate.microsoft.com>
- Mactopia − <http://www.microsoft.com/mac>

V. ♦ Windows Server Update Services − <http://www.microsoft.com/windowsserversystem/updateservices/default.mspx>

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