UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−021

Vulnerabilidades en Microsoft Windows, Internet Explorer, Media Player, Word, PowerPoint, y Exchange

---

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades críticas en Microsoft Windows, Word, PowerPoint, Media Player, Internet Explorer, y Exchange Server. La explotación de estas vulnerabilidades podría permitir un intruso remoto no autenticado para ejecutar código arbitrario o causar una negación de servicio en un sistema vulnerable.

Fecha de Liberación:	13 de Junio de 2006
Ultima Revisión:	13 de Junio 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 Windows Media Player
- Microsoft Internet Explorer
- Microsoft PowerPoint para Windows y Mac OS X
- Microsoft Word para Windows
- Microsoft Office
- Microsoft Works Suite
- Microsoft Exchange Server Outlook Web Access

Para una información más completa, consulte el Resumen de Boletines de Seguridad de Microsoft para Junio 2006.

II. Descripción

Microsoft Security Bulletin Summary for June 2006 soluciona vulnerabilidades en Microsoft Windows, Word, PowerPoint, Media Player, Internet Explorer, y Exchange Server. Mayor información está disponible en las siguientes Notas de Vulnerabilidad del US−CERT:

- **VU#722753 − Vulnerabilidad de Fuente de Ruteo IP en Microsoft Windows**

  Una vulnerabilidad en Microsoft Windows podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−2379)

- **VU#446012 − Vulnerabilidad de corrupción de memoria en apuntado de objeto de Microsoft Word**

  Existe una vulnerabilidad de corrupción de memoria en Microsoft Word que podría permitir a un intruso remoto ejecutar código arbitrario con los privilegios del usuario ejecutando Word.
  (CVE−2006−2492)

- **VU#190089 − Vulnerabilidad de registro malformado en Microsoft PowerPoint**

  Microsoft PowerPoint falla al manejar adecuadamente registros malformados. Esto podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−0022)

- **VU#923236 − Buffer overflow en el manejo de imágenes ART en Microsoft Windows**

  Las rutinas de manejo de imágenes ART en Microsoft Windows son vulnerables a un buffer overflow basado en heap. Esta vulnerabilidad podría permitir a un intruso remoto no autenticado ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−2378)

- **VU#390044 − Vulnerabilidad de corrupción de memoria en Microsoft JScript**

  Microsoft JScript contiene una vulnerabilidad de corrupción de memoria. Esta vulnerabilidad podría permitir a un intruso remoto no autenticado ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−1313)

- **VU#338828 − Vulnerabilidad en el manejo de excepciones en Microsoft Internet Explorer**

Microsoft Internet Explorer falla al manejar adecuadamente condiciones de excepción. Esto podría permitir a un intruso remoto no autenticado ejecutar código arbitrario.
(CVE−2006−2218)

- **VU#417585 − El filtro Microsoft DXImageTransform Light falla al validar una entrada**

  El objeto COM Microsoft DXImageTransform Light falla al validar una entrada, lo cual podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−2383)

- **VU#959049 − Múltiples objetos COM causan corrupción de memoria en Microsoft Internet Explorer**

  Microsoft Internet Explorer (IE) permite la instanciación de objetos COM no designados para uso en el navegador, los cual podía permitir a un intruso remoto ejecutar código arbitrario o causar que falle IE.
  (CVE−2006−2127)

- **VU#136849 − Vulnerabilidad de decodificación UTF−8 en Microsoft Internet Explorer**

  Microsoft Internet Explorer falla al decodificar adecuadamente HTML codificado como UTF−8. Esto podría permitir a un intruso remoto no autenticado ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−2382)

- **VU#909508 − El Motor de Interpretación de Gráficos de Microsoft falla al manejar adecuadamente imágenes WMF**

  El Motor de Interpretación de Gráficos de Microsoft contiene una vulnerabilidad que podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−2376)

- **VU#608020 − Buffer overfloe en el procesamiento PNG en Microsoft Windows Media Player**

  Microsoft Windows Media Player contiene una vulnerabilidad de buffer overflow basado en stack que podría permitir a un intruso remoto no autenticado ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−0025)

- **VU#814644 − El servicio Microsoft Remote Access Connection Manager es vulnerable a un buffer overflow**

  Una vulnerabilidad en Microsoft Remote Access Connection Manager podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable.

(CVE−2006−2371)

- **VU#631516 − Microsoft Routing and Remote Access no reponde al manejo de requerimientos RPC**

  Existe una vulnerabilidad en el servicio Microsoft Windows Routing and Remote Access que podría permitir a un intruso remoto tomar el control remoto del sistema afectado.
  (CVE−2006−2370)

- **VU#138188 − Vulnerabilidad de inyección de secuencia de comandos en Microsoft Outlook Web Access para Exchange Server**

  Existe una vulnerabilidad de inyección de secuencias de comandos en Microsoft Exchange Server ejecutando Outlook Web Access.
  (CVE−2006−1193)

En MS06−027 Microsoft ha liberado actualizaciones para la vulnerabilidad descrita en la Alerta Técnica de Seguridad Cibernética TA06−139A.

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 actualizaciones**

  Microsoft ha producido actualizaciones para estas vulnerabilidades en los Boletines de Seguridad. Las actualizaciones de Microsoft Windows están disponibles en el sitio Microsoft Update.

- **Soluciones temporales**

  Notas de Vulnerabilidades para obtener soluciones temporales.

V. Apéndice

- Proyecto Seguridad en Windows, DSC/UNAM−CERT − http://www.seguridad.unam.mx/windows
- Nota de Vulnerabilidad del US−CERT para las actualizaciones de Microsoft de Junio de 2006 − http://www.kb.cert.org/vuls/byid?searchview&query=ms06−june
- Nota de Vulnerabilidad del US−CERT VU#446012 − http://www.kb.cert.org/vuls/id/446012
- Nota de Vulnerabilidad del US−CERT VU#190089 − http://www.kb.cert.org/vuls/id/190089
- Nota de Vulnerabilidad del US−CERT VU#923236 − http://www.kb.cert.org/vuls/id/923236
- Nota de Vulnerabilidad del US−CERT VU#390044 − http://www.kb.cert.org/vuls/id/390044
- Nota de Vulnerabilidad del US−CERT VU#338828 −

http://www.kb.cert.org/vuls/id/338828
- Nota de Vulnerabilidad del US−CERT VU#417585 − http://www.kb.cert.org/vuls/id/417585
- Nota de Vulnerabilidad del US−CERT VU#136849 − http://www.kb.cert.org/vuls/id/136849
- Nota de Vulnerabilidad del US−CERT VU#909508 − http://www.kb.cert.org/vuls/id/909508
- Nota de Vulnerabilidad del US−CERT VU#722753 − http://www.kb.cert.org/vuls/id/722753
- Nota de Vulnerabilidad del US−CERT VU#959049 − http://www.kb.cert.org/vuls/id/959049
- Nota de Vulnerabilidad del US−CERT VU#138188 − http://www.kb.cert.org/vuls/id/138188
- Nota de Vulnerabilidad del US−CERT VU#608020 − http://www.kb.cert.org/vuls/id/608020
- Nota de Vulnerabilidad del US−CERT VU#814644 − http://www.kb.cert.org/vuls/id/814644
- Nota de Vulnerabilidad del US−CERT VU#631516 − http://www.kb.cert.org/vuls/id/631516
- CVE−2006−2492 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−2492
- CVE−2006−0022 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0022
- CVE−2006−2378 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−2378
- CVE−2006−1313 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1313
- CVE−2006−2218 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−2218
- CVE−2006−2383 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−2383
- CVE−2006−2127 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−2127
- CVE−2006−2382 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−2382
- CVE−2006−2376 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−2376
- CVE−2006−2379 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−2379
- CVE−2006−1193 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−1193
- CVE−2006−0025 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0025
- CVE−2006−2371 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−2371
- CVE−2006−2370 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−2370
- Microsoft Update − https://update.microsoft.com/microsoftupdate
- Asegurando el navegador − 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:

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