UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−007

Vulnerabilidades en Microsoft Windows, Windows Media Player e Internet Explorer

---

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades críticas en Windows, Windows Media Player e Internet Explorer. La explotación de estas vulnerabilidades podrían permitir a un intruso remoto no autenticado ejecutar código arbitrario o causar una negación de servicio en un sistema vulnerable.

Fecha de Liberación:	14 de Febrero de 2006
Ultima Revisión:	14 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

Microsoft Windows	**Cliente de Web**	⊲KB911927
Microsoft Windows	**IME Coreano**	⊲KB901190
Microsoft Windows	**Internet Explorer**	⊲KB910620
Microsoft Windows	**PowerPoint 2000**	⊲KB889167
Microsoft Windows	**TCP/IP**	⊲KB913446
Microsoft Windows	**Windows Media Player**	⊲KB911565
Microsoft Windows	**Windows Media Player**	⊲KB913446

Riesgo

Importante

Problema de Vulnerabilidad

Local y remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Descripción

Los Boletines de Seguridad de Microsoft para Febrero de 2006 solucionan vulnerabilidades en Windows, Windows Media Player, e Internet Explorer. Información más completa está disponible en las siguientes Notas de Vulnerabilidad del US−CERT:

- **VU#312956 − Vulnerabilidad de corrupción de memoria en Microsoft WMF**

  Las aplicaciones de Microsoft fallan adecuadamente al manejar imágenes WMF (Windows Meta File), permitiendo potencialmente a un intruso remoto ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−0020)

- **VU#291396 − Microsoft Windows Media Player es vulnerable a un buffer overflow en rutina de procesamiento de mapa de bits**

  Windows Media Player contiene una vulnerabilidad de buffer overflow que podría permitir a un intruso remoto no autenticado ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−0006)

- **VU#692060 − Buffer overflow en plugin de Microsoft Windows Media Player**

  El plugin de Microsoft Windows Media Player para navegadores distintos a Internet Explorer contiene un buffer overflow, el cual podría permitir a un intruso remoto ejecutar código arbitrario.
  (CVE−2006−005)

- **VU#839284 − Microsoft Windows TCP/IP falla para validar apropiadamente paquetes IGMP**

  Las implementaciones de Microsoft Windows del protocolo TCP/IP fallan al validar apropiadamente paquetes IGMP (Internet Group Management Protocol) lo que causa una condición de negación de servicio.
  (CVE−2006−0021)

II. Impacto

La explotación de estas vulnerabilidades podría permitir a un intruso remoto no autenticado ejecutar código arbitrario con los privilegios de usuario. Si el usuario ha iniciado sesión con privilegios administrativos, le intruso podría tomar el control completo de un sistema afectado. Un intruso podría también ser capaz de causar una negación de servicio.

III. Solución

- **Aplicar actualizaciones**

  Microsoft ha proporcionado las actualizaciones para estas

vulnerabilidades en los Boletines de Seguridad y en el sitio de Microsoft Update.

- **Soluciones temporales**

  Consulte las siguientes Notas de Vulnerabilidad del US−CERT para soluciones temporales.

IV. Apéndice

- Proyecto Seguridad en Windows, DSC/UNAM−CERT − <http://www.seguridad.unam.mx/windows>
- Resumen de Boletines de Seguridad de Microsoft para Febrero de 2006 − <http://www.microsoft.com/technet/security/bulletin/ms06−feb.mspx>
- Nota de Vulnerabilidad del US−CERT VU#312956 − <http://www.kb.cert.org/vuls/id/312956>
- Nota de Vulnerabilidad del US−CERT VU#291396 − <http://www.kb.cert.org/vuls/id/291396>
- Nota de Vulnerabilidad del US−CERT VU#692060 − <http://www.kb.cert.org/vuls/id/692060>
- Nota de Vulnerabilidad del US−CERT VU#839284 − <http://www.kb.cert.org/vuls/id/839284>
- CVE−2006−0020 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0020>
- CVE−2006−0006 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0006>
- CVE−2006−0005 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0005>
- CVE−2006−0021 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0021>
- Microsoft Update − <https://update.microsoft.com/microsoftupdate>

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