UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2005−017

vulnerabilidades en el Procesamiento de Imagenes en Microsoft Windows

---

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades críticas en servicios de interpretación de gráficos de Windows. Un intruso remoto no autenticado que explote estas vulnerabilidades podría ejecutar código arbitrario o causar una negación de servicio en un sistema afectado.

Fecha de Liberación:	8 de Noviembre de 2005
Ultima Revisión:	8 de Noviembre de 2005
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión

Sistemas Afectados

Windows 2000 Todas las versiones	**Motor de interpretación de gráficos**	<KB896424
Windows 2003 Todas las versiones	**Motor de interpretación de gráficos**	<KB896424
Windows XP Todas las versiones	**Motor de interpretación de gráficos**	<KB896424

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Descripción

El Boletín de Seguridad de Microsoft para Noviembre de 2005 soluciona múltiples buffers overflow en las rutinas de procesamiento de imágenes de Windows. Visualizando una imagen creada de forma maliciosa para una aplicación que utilice una rutina vulnerable podría detonar estas vulnerabilidades. Si esta aplicación puede acceder a imágenes desde fuentes remotas, como por ejemplo sitios Web o correo electrónico, la explotación remota es posible.

Para mayor información consulte las siguientes Notas de Vulnerabilidad del US−CER:

- **VU#300549 − Vulnerabilidad de Buffer Overflow en el Motor de Interpretación de Gráficos de Windows**

  Motor de Interpretación de Gráficos de Windows contiene un buffer overflow que podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2005−2123)

- **VU#433341 − Microsoft Windows es vulnerable a un buffer overflow a través de un archivo"WMF" creado de forma maliciosa.**

  Microsoft Windows podría ser vulnerable a una ejecución de código remota a través de un buffer overflow en el manejo del formato de imagen de Metarchivo de Windows.
  (CVE−2005−2124)

- **VU#134756 − Buffer overflow en el API de interpretación de Metarchivo Mejarado**

  Las rutinas de interpretación de imágenes de Formato de Metarchivo Mejorado de Microsoft Windows contienen un buffer overflow que podría permitir a un intruso causar una condición de negación de servicio.
  (CVE−2005−0803)

II. Impacto

Un intruso remoto no autenticado que explote estas vulnerabilidades podría ejecutar código arbitrario con los privilegios del usuario. Si un usuario ha iniciado sesión con privilegios administrativos, el intruso podría tomar el control de un sistema afectado. Un intruso podría ser capaz de causar una negación de servicio.

III. Soluciones

- **Aplicar actualizaciones**

  Microsoft ha proporcionado las actualizaciones para corregir estas vulnerabilidades en el Boletín de Seguridad de Microsoft MS05−053. Estas actualizaciones son también actualizaciones en el sitio de

Microsoft Update.

IV. Apéndice

- Proyecto Seguridad en Windows, DSC/UNAM−CERT − <http://www.seguridad.unam.mx/windows>
- Boletín de Seguridad de Microsoft MS05−053 − <http://www.microsoft.com/technet/security/bulletin/MS05−053.mspx>
- Resumen de Boletines de Seguridad para Noviembre de 2005 − <http://www.microsoft.com/technet/security/bulletin/ms05−nov.mspx>
- Nota de Vulnerabilidad de US−CERT VU#300549 − <http://www.kb.cert.org/vuls/id/300549>
- Nota de Vulnerabilidad de US−CERT VU#433341 − <http://www.kb.cert.org/vuls/id/433341>
- Nota de Vulnerabilidad de US−CERT VU#134756 − <http://www.kb.cert.org/vuls/id/134756>
- 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