UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−001

Vulnerabilidad en el motor de interpretación de gráficos en WMF

El CERT/UNAM−CERT, a través de sus equipos de respuesta a incidentes de Seguridad en Cómputo, informan que Microsoft ha publicado el día de hoy una actualización correspondiente a la vulnerabilidad de seguridad previamente conocida en el área de código de WMF (Windows Meta File) en el sistema operativo Windows.

Esta vulnerabilidad se encuentra descrita ampliamente en el boletín UNAM−CERT 2005−018 "Buffer Overflow en el Manejo de Metarchivos en Microsoft Windows"

De acuerdo al Boletín de Seguridad de Microsoft MS06−01 Microsoft publica una actualización para la vulnerabilidad descrita en el Boletín UNAM−CERT 2005−018.

Fecha de Liberación:	5 de Enero de 2006
Ultima Revisión:	5 de Enero de 2006
Fuente:	Microsoft PSIRT, CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión.

Sistemas Afectados

Windows 2000 SP4	**Metarchivo de Windows**	<KB912919
Windows 2003 −	**Metarchivo de Windows**	<KB912919
Windows 2003 Edición x64	**Metarchivo de Windows**	<KB912919
Windows 2003 Service Pack 1	**Metarchivo de Windows**	<KB912919
Windows 2003 Service Pack 1 para Sistemas Basados en Itanium	**Metarchivo de Windows**	<KB912919
Windows 2003 Sistemas Basados en	**Metarchivo de Windows**	<KB912919

Itanium		
Windows XP Profesional Edición x64	**Metarchivo de Windows**	KB912919
Windows XP Service Pack 1	**Metarchivo de Windows**	KB912919
Windows XP Service Pack 2	**Metarchivo de Windows**	KB912919

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Ejecución Remota de Código

I. **Descripción**

- **Vulnerabilidad en el motor de interpretación de gráficos.**

  Existe una vulnerabilidad de ejecución remota de código en el motor de Interpretación de Gráficos debido a la forma en que maneja imágenes WMF (Windows Metafile). Un intruso que explote esta vulnerabilidad construyendo una imagen WMF creada de forma maliciosa podría potencialmente permitir la ejecución remota de código si un usuario visita el sitio Web malicioso o abre un archivo adjunto malicioso.

II. **Impacto**

Un intruso que haya explotado satisfactoriamente esta vulnerabilidad podría tomar el control completo del sistema afectado.

III. **Solución**

Aplicar actualización:

- Microsoft Windows 2000 Service Pack 4 – Descargar la actualización
- Microsoft Windows XP Service Pack 1 y Microsoft Windows XP Service Pack 2 – Descargar la actualización
- Microsoft Windows XP Professional x64 Edition – Descargar la actualización
- Microsoft Windows Server 2003 y Microsoft Windows Server 2003 Service Pack 1 – Descargar la actualización
- Microsoft Windows Server 2003 para sistemas Itanium y Microsoft Windows Server 2003 con SP1 para sistemas Itanium – Descargar la actualización
- Microsoft Windows Server 2003 x64 Edition – Descargar la actualización
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), y Microsoft Windows Millennium Edition (ME) – Ver la sección del

FAQ para más detalles de esta versión de sistema operativo.

IV. Apéndice

- Boletín de Seguridad UNAM−CERT 2005−018 "Buffer Overflow en el Manejo de Metarchivos en Microsoft Windows" − http://www.cert.org.mx/boletin/?vulne=4964
- Boletín de Seguridad de Microsoft MS06−001 − http://www.microsoft.com/technet/security/Bulletin/MS06−001.mspx
- Boletín de Seguridad US−CERT − http://www.us−cert.gov/cas/techalerts/TA06−005A.html

---

El Departamento de Seguridad en Cómputo/UNAM−CERT agradece el apoyo en la traducción, elaboración y revisión de éste Documento a:

- Luis Fernando Fuentes Serrano (lfuentes at seguridad dot unam dot mx)
- 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