

UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA-UNAM

Boletín de Seguridad UNAM-CERT-2007-012

Actualización de Microsoft para vulnerabilidad en cursor animado de Windows

Microsoft ha liberado actualizaciones en la forma en como Microsoft Windows maneja archivos de imagen. Una solución para la vulnerabilidad de buffer overflow de cursor animado (VU#191609) está incluida en estas actualizaciones.

Fecha de Liberación: 3 de Abril de 2007

Ultima Revisión: 3 de Abril de 2007

Fuente: CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como foros y listas de discusión.

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Ejecución Remota de Código

I. Sistemas Afectados

Los sistemas Microsoft Windows 2000, XP, Server 2003 y Vista son afectados. Las aplicaciones que proporcionan vectores de ataques incluyen:

- ◆ Microsoft Internet Explorer
- ◆ Microsoft Outlook
- ◆ Microsoft Outlook Express
- ◆ Microsoft Windows Mail
- ◆ Microsoft Windows Explorer

II. Descripción

Microsoft ha liberado el Boletín de Seguridad MS07-017 para corregir vulnerabilidades en la forma en que Microsoft Windows maneja archivos de imagen. Esta actualización incluye una solución para la vulnerabilidad de buffer overflow de pila en la cabecera del cursor animado ANI (VU#191609).

Para obtener mayor información sobre la vulnerabilidad de buffer overflow en el cursor animado puede consultar la Nota de Vulnerabilidad VU#191609 y el Boletín de Seguridad **boletin-UNAM-CERT-2007-011**. Consulte el Boletín de Seguridad de Microsoft MS07-017 para mayor información sobre otras vulnerabilidades.

III. Impacto

Aplicando estas actualizaciones mitigarán la vulnerabilidad descrita en el Boletín de Seguridad **boletin-UNAM-CERT-2007-011**. El impacto de explotar esta vulnerabilidad es que un intruso remoto no autenticado podría ejecutar código arbitrario o causar una condición de negación de servicio.

IV. Solución

Instalar actualizaciones de Microsoft

Microsoft ha liberado actualizaciones para ésta y otras vulnerabilidades en el procesamiento de imágenes en el Boletín de Seguridad de Microsoft MS07-017.

Se debe hacer notar que esto es solo parte de la liberación de actualizaciones de seguridad de Microsoft para Abril de 2007. De acuerdo con Microsoft:

Microsoft actualizará este resumen de boletines con cualquier otro boletín de seguridad que se libere el 10 de Abril o en cualquier otro día del mes, como se considere apropiado.

Los administradores de sistemas podrían considerar utilizar un sistema de distribución de actualizaciones como Windows Server Update Services (WSUS).

Consulte el Boletín de Seguridad **boletin-UNAM-CERT-2007-011** y la Nota de Vulnerabilidad VU#191609 para mayor información sobre soluciones temporales que podrían reducir las opciones de explotación hasta que las actualizaciones puedan ser aplicadas.

V. Referencias

- ◆ Proyecto Seguridad en Windows, DSC/UNAM-CERT –
<<http://www.seguridad.unam.mx/windows>>
- ◆ Alerta Técnica de Seguridad Cibernética del US-CERT TA07-089A –
<<http://www.us-cert.gov/cas/techalerts/TA07-089A.html>>
- ◆ Nota de Vulnerabilidad VU#191609 –
<<http://www.kb.cert.org/vuls/id/191609>>
- ◆ Boletín de Seguridad de Microsoft MS07-017 –
<<http://www.microsoft.com/technet/security/bulletin/ms07-017.msp>>

UNAM-CERT

- ◆ Aviso de Seguridad de Microsoft (935423) –
<<http://www.microsoft.com/technet/security/advisory/935423.msp>>
 - ◆ Resumen de Boletines de Seguridad de Microsoft para Abril 2007 –
<<http://www.microsoft.com/technet/security/bulletin/ms07-apr.msp>>
 - ◆ Microsoft Security Response Center Blog –
<<http://blogs.technet.com/msrc/search.aspx?q=935423>>
 - ◆ Windows Server Updates Services –
<<http://www.microsoft.com/windowsserversystem/updateservices/default.msp>>
-

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