UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2007−011

Buffer overflow de pila en cabeceras ANI de Microsoft Windows

---

Actualmente está siendo explotada una vulnerabilidad no actualizada de buffer overflow en la forma en como Microsoft Windows maneja archivos de cursor animados.

Fecha de Liberación:	30 de Marzo de 2007
Ultima Revisión:	30 de Marzo 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

Manejo de Peticiones

I. Sistemas Afectados

Son afectadas las versiones de Windows 2000, Windows Server 2003 y Windows Vista. Las aplicaciones que proporcionan vectores de ataques incluyen:

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

II. Descripción

Existe un buffer overflow de pila en el código que Microsoft Windows utiliza para procesar archivos de cursor animado. Específicamente, Microsoft Windows falla al validar adecuadamente el tamaño de la cabecera de un archivo de cursor animado.

Los archivos de cursor animado pueden ser incluidos con archivos HTML. Por ejemplo, un sitio Web puede utilizar un archivo de cursor animado para especificar el icono que el apuntador del ratón debería utilizar cuando pase sobre un hipervínculo. Debido a esto, pueden ser utilizadas páginas Web maliciosas y mensajes de correo HTML para explotar esta vulnerabilidad. Además, los archivos de cursor animados son analizados automáticamente por el Explorador de Windows cuando la carpeta que los contiene es abierta o el archivo es utilizado como un cursor. Debido a esto, abriendo un directorio que contenga un archivo de cursor animado malicioso también activará la vulnerabilidad.

Se debe hacer notar que el Explorador de Windows procesará archivos de cursor animados con distintas extensiones, como por ejemplo, .ani, .cur, or .ico. Además, Windows identificará como válidos los archivos de cursor animado en documentos HTML independientemente de su extensión.

La vulnerabilidad está siendo explotada activamente.

Más información está disponible en la Nota de Vulnerabilidad VU#191609.

III. Impacto

Un intruso remoto no autenticado podría ser capaz de ejecutar código arbitrario. La explotación podría ocurrir cuando los usuarios hagan clic sobre un vínculo malicioso, lean o reenvíen un correo electrónico HTML malicioso, o accedan a una carpeta que contenga un archivo de cursor animado malicioso.

IV. Solución

Hasta que una actualización sea liberada, puede consultar la sección *Solution* de la Nota de Vulnerabilidad VU#191609 para obtener las soluciones temporales más recientes.

V. Referencias

- Nota de Vulnerabilidad VU#191609 − <http://www.kb.cert.org/vuls/id/191609>
- Microsoft Security Advisory (935423) − <http://www.microsoft.com/technet/security/advisory/935423.mspx>
- Unpatched Drive−By Exploit Found On The Web − <http://www.avertlabs.com/research/blog/?p=230>
- TROJ_ANICHMOO.AX − Description and Solution − <http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FANICMOO%2EAX

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