UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−005

Buffer overflow en lista de reproducción de Winamp

American Online ha liberado Winamp 5.13 para corregir una vulnerabilidad de buffer overflow. La explotación de ésta vulnerabilidad podría permitir a un intruso remoto ejecutar código arbitrario con privilegios del usuario.

Fecha de Liberación:	2 de Febrero de 2006
Ultima Revisión:	3 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 todas las versiones	**Winamp**	<=5.12

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Buffer Overflow

I. **Descripción**

Winamp es un reproductor de multimedia muy utilizado para reproducir archivos MP3. Winamp 5.13 resuelve una vulnerabilidad de buffer overflow en la forma en como se manejan los archivos de listas de reproducción. Detalles de la vulnerabilidad están disponibles en la siguiente Nota de Vulnerabilidad:

- **VU#604745** − Winamp falla al no manejar apropiadamente listas de reproducción con nombres de equipos largos.

  Winamp contiene una vulnerabilidad de buffer overflow cuando procesa una lista de reproducción que especifica un nombre de equipo largo. Esto puede provocar que un intruso no autenticado ejecute código arbitrario en un sistema vulnerable.

II. Impacto

Convenciendo a un usuario para que abra un archivo especialmente diseñado, un intruso no autenticado podría ejecutar código arbitrario con privilegios del usuario. Winamp puede abrir un archivo automáticamente sin la interacción del usuario como resultado de solo acceder a una página Web u otro documento en HTML.

III. Solución

Actualizar Winamp a la versión 5.13

- Descargar actualización

IV. Apéndice

- Nota de Vulnerabilidad del US−CERT − <http://www.kb.cert.org/vuls/id/604745>
- CVE−2006−0476 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0476>
- Base de Datos Nacional de Vulnerabilidades (CVE−2006−0476) − <http://nvd.nist.gov/nvd.cfm?cvename=CVE−2006−0476>
- WINAMP.COM | Player | Version History − <http://www.winamp.com/player/version_history.php>
- WINAMP.COM | Player − <http://www.winamp.com/player>

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

- Juan Lopez Morales (jlopez at correo dot seguridad dot unam dot mx)
- Luis Fernando Fuentes Serrano (lfuentes 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