UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−031

Vulnerabilidad en el control ActiveX WebViewFolderIcon de Microsoft Internet Explorer

---

El control ActiveX WebViewFolderIcon de Microsoft Windows contiene una vulnerabilidad de overflow de entero que podría permitir a un intruso remoto ejecutar código arbitrario.

Fecha de Liberación:	27 de Septiembre de 2006
Ultima Revisión:	27 de Septiembre de 2006
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

- Microsoft Windows
- Microsoft Internet Explorer

II. Descripción

El control ActiveX WebViewFolderIcon de Microsoft Windows contiene una vulnerabilidad de overflow de entero. Un intruso podría explotar esta vulnerabilidad mediante Internet Explorer de Microsoft o cualquier otra aplicación que utilice el control WebViewFolderIcon. Más información se puede encontrar en la Nota de Vulnerabilidad del US−CERT VU#753044.

III. Impacto

Convenciendo a un usuario de que abra un archivo especialmente diseñado en HTML, tal como páginas Web o mensajes de correo electrónico en HTML, un intruso podría ejecutar código arbitrario con privilegios del usuario que esté ejecutando el programa en el equipo con el control WebViewFolderIcon.

IV. Solución

Microsoft no ha liberado una actualización para ésta vulnerabilidad. Considere las siguientes soluciones temporales y mejores prácticas:

- **Deshabilitar el control ActiveX WebViewFolderIcon**

  Para proteger contra la vulnerabilidad específica, deshabilite el control WebViewFolderIcon estableciendo el bit de desactivación para el siguiente CLSID:

  {844F4806−E8A8−11d2−9652−00C04FC30871}

  Mayor información sobre como establecer el bit de desactivación está disponible en el Documento de Soporte de Microsoft 240797.

- **Desactivar ActiveX**

  Para protegerse contra ésta y otras vulnerabilidades en Active X y COM, deshabilite ActiveX en la Zona de Internet y cualquier otra zona que podría ser utilizada por un intruso. Las instrucciones para deshabilitar ActiveX en la Zona de Internet pueden ser encontradas en el documento "Asegurando tu navegador Web (en inglés)" y el FAQ Scripts de Web Maliciosos (en inglés).

- **Establecer la lectura de correos electrónicos en texto plano**

  Para protegerse contra ésta y otras vulnerabilidades que requieren que una víctima cargue un documento HTML malicioso configure los clientes de correo electrónico obtengan los correos en texto plano.

- **No hacer clic en vínculos no solicitados**

  Para protegerse contra ésta y otras vulnerabilidades que requieren que una víctima cargue un documento HTML malicioso no haga clic en vínculos no solicitados o poco confiables.

  Con el propósito de convencer a los usuarios a visitar sus sitios, los intrusos a menudo utilizan codificación URL, variaciones de direcciones IP, URLs largos, palabras mal escritas de forma intencional y otras técnicas para crear vínculos engañosos. No se debe hacer clic en vínculos no solicitados recibidos en correos electrónicos, mensajes instantáneos, foros Web o canales IRC. Escriba directamente el URL en el navegador para evitar estos vínculos engañosos. Mientras estas son generalmente buenas prácticas de seguridad, siguiendo estos comportamientos no prevendrá la explotación de ésta vulnerabilidad en

todos los casos, particularmente si un sitio confiado ha sido comprometido o permite cross−site scripting.

V. Referencias

- Proyecto Seguridad en Windows, DSC/UNAM−CERT − <http://www.seguridad.unam.mx/windows
- Nota de Vulnerabilidad del US−CERT VU#753044 − <http://www.kb.cert.org/vuls/id/753044>
- Asegurando tu navegador Web (en inglés) − <http://www.us−cert.gov/reading_room/securing_browser/>
- FAQ Scripts de Web Maliciosos (en inglés) − <http://www.cert.org/tech_tips/malicious_code_FAQ.html>
- CVE−2006−3730 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−3730>
- Documento de Soporte de Microsoft 240797 (en inglés) − <http://support.microsoft.com/kb/240797>

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)
- Juan Lopez Morales (jlopez at correo dot 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