UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−030

Buffer oveflow en VML de Internet Explorer

Microsoft Internet Explorer (IE) falla al manejar etiquetas VML (Vector Markup Language). Esto crea una vulnerabilidad de buffer overflow que podría permitir a un intruso remoto ejecutar código arbitrario.

Fecha de Liberación:	20 de Septiembre de 2006
Ultima Revisión:	26 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

Microsoft Internet Explorer contiene un buffer overflow de stack en el código que maneja VML. Más información está disponible en la Nota de Vulnerabilidad VU#416092 y el Aviso de Seguridad de Microsoft (925568).

Se debe hacer notar que ésta vulnerabilidad está siendo explotada.

III. Impacto

Convenciendo a un usuario de que abra un documento HTML creado de forma maliciosa, como una página Web o un mensaje de correo en formato HTML, un intruso remoto podría ejecutar código arbitrario con los privilegios del usuario ejecutando IE.

IV. Solución

- **Aplicar una actualización de Microsoft Corp.**

  Microsoft ha proporcionado una actualización para corregir ésta vulnerabilidad en el Boletín de Seguridad de Microsoft MS06−055.

  Ésta actualización está disponible en el sitio Microsoft Update.

  Los administradores de sistemas podrían considerar utilizar (WSUS).

- **Deshabilitar el soporte de VML**

  El Aviso de Seguridad de Microsoft (925568) sugiere las siguientes técnicas para deshabilitar el soporte de VML:

  - Quitar el registro para Vgx.dll en Windows XP Service Pack; Windows XP Service Pack 2; Windows Server 2003 y Windows Server 2003 Service Pack 1.
  - Modificar la Lista de Control de Acceso en Vgx.dll para que sea más restrictivo.
  - Configurar Internet Explorer 6 para Microsoft Windows XP Service Pack 2 para deshabilitar Comportamientos Binarios y de Scripts en la zona de seguridad de Internet e Intranet Local.

  Deshabilitar el soporte para VML podría causar que los sitios Web que utilicen VML funcionen de forma inapropiada.

- **Impacto de soluciones temporales**

  Las aplicaciones que proporcionan VML no trabajarán una vez que se haya de−registrado vgx.dll.

  La actualización de seguridad no registra automáticamente a vgx.dll por lo que cualquier aplicación que proporcione VML no trabajará hasta que vgx.dll haya sido registrado nuevamente. Para volver a registrar vgx.dll realice los siguientes pasos:

  1. Haga clic en Inicio, Ejecutar y escriba "%SystemRoot%\System32\regsvr32.exe" "%CommonProgramFiles%\Microsoft Shared\VGX\vgx.dll", y después haga clic en Aceptar.
  2. Aparecerá un cuadro de diálogo para confirmar que el proceso de registro ha sido satisfactorio. Haga clic en Aceptar para cerrar el cuadro de diálogo.

De igual forma, si se han modificado las ACLs para el archivo vgx.dll se deben volver a establecerse a su estado original debido a que pueden causar que está actualización de seguridad falle.

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

  El Aviso de Seguridad de Microsoft (925568) sugiere configurar Microsoft Outlook y Outlook Express para que se lean lo mensajes de correo electrónico en formato de texto plano.

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

  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 VU#416092 − <http://www.kb.cert.org/vuls/id/416092>
- Asegurando tu navegador Web − <http://www.us−cert.gov/reading_room/securing_browser/#Internet_Explorer>
- Aviso de Seguridad de Microsoft (925568) − <http://www.microsoft.com/technet/security/advisory/925568.mspx>
- CVE−2006−3866 − <http://www.cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−3866>

VI. Revisión histórica

- **19 de Septiembre:** Liberación original
- **26 de Septiembre:** Se agregaron los puntos Aplicar una actualización de Microsoft Corp. e Impacto de soluciones temporales a la sección Solución.

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