UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2007−005

Actualizaciones de Microsoft para múltiples vulnerabilidades

Microsoft ha liberado actualizaciones para solucionar vulnerabilidades en Microsoft Windows, Internet Explorer, Office, Works, Malware Protection Engine, Visual Studio y Step−by−Step Interactive Training. La explotación de estas vulnerabilidades podría permitir a intruso remoto no autenticado ejecutar código arbitrario o causar una negación de servicio en un sistema vulnerable.

Fecha de Liberación:	13 de Febrero de 2007
Ultima Revisión:	13 de Febrero 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

Local y remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Sistemas afectados

- Microsoft Windows
- Microsoft Internet Explorer
- Microsoft Office
- Microsoft Works
- Microsoft Malware Protection Engine
- Microsoft Visual Studio
- Microsoft Step−by−Step Interactive Training

II. Descripción

Microsoft ha liberado actualizaciones para solucionar vulnerabilidades que afectan Microsoft Windows, Internet Explorer, Office, Works, Malware Protection Engine, Visual Studio, y Step−by−Step Interactive Training como parte de su Resumen de Boletines de Seguridad para Febrero de 2007. La más severa de las vulnerabilidades podría permitir a un intruso no autenticado ejecutar código arbitrario o causar una negación de servicio en un sistema vulnerable.

Algunas de las actualizaciones liberadas para Microsoft Office solucionan vulnerabilidades que están siendo explotadas activamente. Para mayor información, consulte las Notas de Vulnerabilidad.

Mayor información sobre las vulnerabilidades solucionadas por estas actualizaciones está disponible en la Base de Datos de Notas de Vulnerabilidades.

III. Impacto

Un intruso remoto no autenticado podría ejecutar código arbitrario en un sistema vulnerable. Un intruso podría también ser capaz de causar una negación de servicio.

IV. Solución

- Aplicar actualizaciones de Microsoft

  Microsoft ha proporcionado actualizaciones para estas vulnerabilidades en los Boletines de Seguridad de febrero de 2007. Los Boletines de Seguridad describen cualquier problema conocido relacionado con las actualizaciones. Note cualquier problema descrito en los Boletines y pruebe cualquier efecto adverso en su ambiente.

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

V. Referencias

- Proyecto Seguridad en Windows, DSC/UNAM−CERT − <http://www.seguridad.unam.mx/windows>
- Nota de Vulnerabilidades del US−CERT para Actualizaciones de de Febrero de 2007 − <http://www.kb.cert.org/vuls/byid?searchview&query=ms07−feb>
- Asegurando tu navegador Web − <http://www.us−cert.gov/reading_room/securing_browser/>
- Resumen de Boletines de Seguridad para Febrero de 2007 − <http://www.microsoft.com/technet/security/bulletin/ms07−feb.mspx>
- Microsoft Update − <https://update.microsoft.com/microsoftupdate/>
- Microsoft Office Update − <http://officeupdate.microsoft.com/>
- Windows Server Update Services − <http://www.microsoft.com/windowsserversystem/updateservices/default.mspx>

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