UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2007−023

Actualizaciones de Microsoft para múltiples vulnerabilidades

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades críticas en Microsoft Windows, Microsoft Visual Studio, Microsoft Windows Services for Unix, y Microsoft MSN Messenger. La explotación de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar código arbitrario o causar una negación de servicio en un sistema vulnerable.

Fecha de Liberación:	11 de Septiembre de 2007
Ultima Revisión:	12 de Septiembre 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

Múltiples vulnerabilidades

I. **Sistemas afectados**

- Microsoft Windows
- Microsoft Visual Studio
- Microsoft Windows Services for Unix
- Microsoft MSN Messenger

II. **Descripción**

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades críticas en Microsoft Windows, Microsoft Visual Studio, Microsoft Windows Services for Unix, y Microsoft MSN Messenger como parte de su Resumen de Boletines de Seguridad para Septiembre 2007. La más severa de las vulnerabilidades

podría permitir a un atacante remoto no autenticado ejecutar código arbitrario o causar una negación de servicio en un sistema vulnerable.

Para mayor información sobre las vulnerabilidades solucionan estas actualizaciones disponibles en la Base de datos de las Notas de Vulnerabilidad.

III. Impacto

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

IV. Solución

Microsoft ha proporcionado actualizaciones para estas vulnerabilidades es los de boletines de seguridad de septiembre de 2007. Los boletines de seguridad describen cualquier problema conocido relacionado con las actualizaciones. Note cualquier problema conocido descrito en los Boletines y pruebe cualquier afectación potencialmente adversa en su ambiente.

Los administradores de sistemas podrían desear utilizar un sistema de distribución automatizado de actualizaciones como WSUS (Windows Server Update Services).

V. Referencias

- Proyecto Seguridad en Windows, DSC/UNAM−CERT − <http://www.seguridad.unam.mx/windows>
- Notas de Vulnerabilidad del US−CERT para actualizaciones para Septiembre de 2007 − <http://www.kb.cert.org/vuls/byid?searchview&query=ms07−sep>
- Asegurando tu navegador Web − <http://www.us−cert.gov/reading_room/securing_browser/>
- Resumen de Boletines de Seguridad de Microsoft para Septiembre de 2007 − <http://www.microsoft.com/technet/security/bulletin/ms07−sep.mspx>
- Microsoft Update − <https://update.microsoft.com/microsoftupdate/>
- 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)

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