UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2007−002

Actualizaciones de Microsoft para múltiples vulnerabilidades

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades críticas en Microsoft Windows, Internet Explorer, Outlook y Excel. 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:	9 de Enero de 2007
Ultima Revisión:	9 de Enero 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

Ejecución remota de código y negación de servicio

I. **Sistemas afectados**

- Microsoft Windows
- Microsoft Internet Explorer
- Microsoft Outlook
- Microsoft Excel for Windows and Mac OS X

II. **Descripción**

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades que afectan Microsoft Windows, Internet Explorer, Outlook y Excel como parte del Resumen de Boletines de Seguridad para Enero de 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.

Se debe hacer notar que las versiones de Windows y Mac OS X son afectadas por las vulnerabilidades descritas en el Boletín de Seguridad MS07−002.

Para obtener mayor información sobre las vulnerabilidades cubiertas por estas actualizaciones está disponible en la Base de Datos de Notas de Vulnerabilidades.

III. Impacto

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

IV. Solución

- **Aplicar actualizaciones de Microsoft.**

  Microsoft ha proporcionado actualizaciones para estas vulnerabilidades en para Enero 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 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>
- Notas de Vulnerabilidad del US−CERT de Actualizaciones de Microsoft para Enero de 2007 − <http://www.kb.cert.org/vuls/byid?searchview&query=ms07−jan>
- Asegurando su navegador Web (en inglés) − <http://www.us−cert.gov/reading_room/securing_browser/>
- Resumen de Boletines de Seguridad de Microsoft para Enero de 2007 − <http://www.microsoft.com/technet/security/bulletin/ms07−jan.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)

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