UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2007−024

Actualizaciones de Microsoft para múltiples vulnerabilidades

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades críticas en Microsoft Windows, Microsoft Internet Explorer, Microsoft Outlook Express y Windows Mail, Microsoft Office, Microsoft Office para Mac y Microsoft SharePoint. La explotación de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar código de su elección o causar una negación de servicio en el sistema vulnerable.

Fecha de Liberación:	9 de Octubre de 2007
Ultima Revisión:	9 de Octubre 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 Window
- Microsoft Internet Explorer
- Microsoft Outlook Express y Windows Mail
- Microsoft Office
- Microsoft Office para Mac
- Microsoft SharePoint

II. Descripción

Microsoft ha liberado actualizaciones para solucionar vulnerabilidades que afectan a Microsoft Windows, Microsoft Internet Explorer, Microsoft Outlook Express y Windows Mail, Microsoft Office, Microsoft Office para Mac, y Microsoft SharePoint como parte de su Resumen de Boletines de Seguridad de Microsoft para Octubre de 2007. La más severa de las vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar código de su elección o causar una negación de servicio en un sistema vulnerable.

Para mayor información sobre las vulnerabilidad solucionadas por estas actualizaciones puede consultar la Base de Datos de Notas de Vulnerabilidad.

III. Impacto

Un atacante remoto no autenticado podría ejecutar código de su elección en un sistema vulnerable. Un atacante 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 octubre de 2007. Los boletines de seguridad describen cualquier problema conocido relacionado con las actualizaciones. Se recomienda a los administradores notar cualquier problema conocido descrito en los Boletines y probar 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 de Microsoft de Octubre de 2007 − <http://www.kb.cert.org/vuls/byid?searchview&query=ms07−oct>
- Resumen de Boletines de Seguridad de Microsoft para Octubre de 2007 − <http://www.microsoft.com/technet/security/bulletin/ms07−oct.mspx>
- Microsoft Update − <https://update.microsoft.com/microsoftupdate/>
- Windows Server Update Services − <http://www.microsoft.com/windowsserversystem/updateservices/default.mspx>
- Asegurando tu navegador Web (inglés) − <http://www.cert.org/tech_tips/securing_browser/>
- Mactopia − <http://www.microsoft.com/mac/>

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