UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2007−018

Actualizaciones de Microsoft para Múltiples Vulnerabilidades

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades críticas en Microsoft Windows, Windows Secure Channel, Internet Explorer, Win32 API, Windows Mail y Outlook Express. 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:	12 de Junio de 2007
Ultima Revisión:	12 de Junio 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 Internet Explorer
- Microsoft Visio
- Microsoft Windows Mail
- Microsoft Outlook Express
- Microsoft Secure Channel
- Win32 API

II. Descripción

Microsoft ha liberado actualizaciones para solucionar vulnerabilidades que afectan a Microsoft Windows, Windows Secure Channel, Internet Explorer, Win32 API, Visio, Outlook Express y Windows Mail como parte de su Resumen de Boletines de Seguridad para Junio 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.

Para mayor información sobre las vulnerabilidades solucionadas por estas actualizaciones puede consultar 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 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 Junio de 2007. Los Boletines de Seguridad describen cualquier problema 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 de Microsoft de Junio de 2007 − <http://www.kb.cert.org/vuls/byid?searchview&query=ms07−jun>
- Asegurando tu navegador Web − <http://www.us−cert.gov/reading_room/securing_browser/>
- Resumen de Boletines de Seguridad de Microsoft para Junio de 2007 − <http://www.microsoft.com/technet/security/bulletin/ms07−jun.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)

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