UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2007−017

Actualizaciones de Microsoft para Múltiples Vulnerabilidades

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades críticas en Microsoft Windows, Internet Explorer, Office, Exchange, CAPICOM y BizTalk. La explotación de estas vulnerabilidades podría permitir a un intruso remoto no autenticado ejecutar código arbitrario o causar una negación de servicio en un sistema vulnerable.

Fecha de Liberación:	8 de Mayo de 2007
Ultima Revisión:	8 de Mayo 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 Windows Server
- Microsoft Internet Explorer
- Microsoft Office para Windows y Mac OS X
- Microsoft Exchange
- Microsoft CAPICOM
- Microsoft BizTalk

II. Descripción

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades que afectan a Microsoft Windows, Internet Explorer, Office, Exchange, CAPICOM y BizTalk como parte del Resumen de Boletines de Seguridad de Microsoft para Mayo 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.

Adicionalmente una vulnerabilidad previamente revelada que soluciona una vulnerabilidad en el RPC del DNS de Microsoft.

Más información sobre las vulnerabilidades solucionadas por estas actualizaciones está disponible a través de la Base de Datos de Notas de Vulnerabilidades del US−CERT.

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 como parte de su Resumen de Boletines de Seguridad de Microsoft para Mayo de 2007. Los Boletines de Seguridad describen cualquier problema relacionado con las actualizaciones. Note cualquier problema descrito en los Boletines y pruebe cualquier efecto potencial adverso en su ambiente de cómputo.

Los administradores de sistemas podrían considerar utilizar un 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 para actualizaciones de Microsoft de Mayo de 2007 − <http://www.kb.cert.org/vuls/byid?searchviewa>>
- Alerta de seguridad Técnica TA07−103A: Microsoft Windows DNS RPC Buffer Overflow − <http://www.us−cert.gov/cas/techalerts/TA07−103A.html>
- Resumen de Boletines de Seguridad de Microsoft para Mayo 2007 − <http://www.microsoft.com/technet/security/bulletin/ms07−may.mspx>
- Microsoft Update − <https://update.microsoft.com/microsoftupdate/>
- Windows Server Update Services − <http://www.microsoft.com/windowsserversystem/updateservices/default.mspx>
- Asegurando tu navegador Web (En inglés) − <http://www.us−cert.gov/reading_room/securing_browser/>
- Microsoft Office Update − <http://officeupdate.microsoft.com/>

- Microsoft Office para Mac Update − <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:

- Juan Lopez Morales (jlopez 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