UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−016

Vulnerabilidades en Microsoft Windows y Microsoft Exchange Server

---

Microsoft ha liberado actualizaciones críticas para Microsoft Windows y para Microsoft Exchange Server. La explotación de estas vulnerabilidades podría permitir a un intruso la ejecución de código remoto o provocar una Negación de Servicios en el sistema vulnerable.

Fecha de Liberación: 9 de Mayo de 2006

Ultima Revisión: 9 de Mayo de 2006

Fuente:

Sistemas Afectados

Microsoft Windows	**Microsoft Exchange Server**	== Microsoft Exchange Server
Microsoft Windows	**Microsoft Windows**	== Microsoft Windows

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. **Descripción**

Microsoft ha publicado sus boletines de seguridad correspondientes al mes de Mayo del 2006 alertando sobre vulnerabilidades en Microsoft Windows y en Microsoft Enchange Server. La información completa se encuentra disponible a

través de las siguientes Notas de Vulnerabilidad del US−CERT:

VU#303452 − Fallas en Microsoft Exchange en la manera en que maneja las propiedades vCal e iCal.

Microsoft Exchange Server no maneja adecuadamente las propiedades de vCal e iCal de los correos electrónicos. La explotación de esta vulnerabilidad puede permitir que un intruso ejecute código arbitrario en el servidor de correo. (CVE−2006−0027)

VU#945060 − Los productos de Adobe Flash contienen múltiples vulnerabilidades.

Varias vulnerabilidades encontradas en los productos de Macromedia Flash pueden permitir a un intruso la ejecución de código remoto sobre el sistema vulnerable. (CVE−2006−0024)

VU#146284 − Fallas en Macromedia Flash Player para validar apropiadamente el identificador de los archivos "SWF".

Una vulnerabilidad de buffer overflow en algunas versiones de Macromedia Flash Player puede permitir la ejecución de código remoto sobre el sistema vulnerable.

II. Impacto

Ejecución de código remoto. Además, un intruso puede ser capaz de causar una Negación de servicio.

III. Solución

Aplicar la actualización correspondiente.

Microsoft ha publicado las actualizaciones de seguridad para estas vulnerabilidades en su boletín de seguridad correspondiente. También están disponibles a través de su servicio de Microsoft Windows Update.

IV. Apéndice

- Proyecto Seguridad en Windows, DSC/UNAM−CERT − <http://www.seguridad.unam.mx/windows>
- Resumen de Boletines de Seguridad de Microsoft para Mayo de 2006 − http://www.microsoft.com/technet/security/bulletin/ms06−may.mspx
- Alerta Técnica de Ciberseguridad TA06−075A − http://www.us−cert.gov/cas/techalerts/TA06−075A.html
- Nota de Vulnerabilidada del US−CERT VU#303452 − http://www.kb.cert.org/vuls/id/303452
- Nota de Vulnerabilidada del US−CERT VU#945060 − http://www.kb.cert.org/vuls/id/945060
- Nota de Vulnerabilidada del US−CERT VU#146284 − http://www.kb.cert.org/vuls/id/146284
- CVE−2006−0027 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0027
- CVE−2006−0024 −

http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0024
- CVE−2005−2628 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2005−2628
- Microsoft Update − https://update.microsoft.com/microsoftupdate

---

El Departamento de Seguridad en Cómputo/UNAM−CERT agradece el apoyo en la traducción, elaboración y revisión de éste Documento a:

- Luis Fernando Fuentes Serrano (lfuentes at seguridad dot unam dot mx)
- 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