UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA-UNAM

Boletin de Seguridad UNAM-CERT-2010-012

Actualizaciones de Microsoft para múltiples Vulnerabilidades

Microsoft ha liberado boletines de seguridad sobre múltiples vulnerabilidades en Microsoft Outlook Express, Microsoft Windows Mail, Microsoft Windows Live Mail, Microsoft Office y Microsoft Visual Basic for Applications.

Fecha de Liberación: 13 de Mayo de 2010

Ultima Revisión: 18 de Mayo de 2010

Fuente: CERT/CC

Riesgo

Crítico

Problema de Vulnerabilidad

Local y remoto

Tipo de Vulnerabilidad

Ejecución Remota de Código

I. Sistemas Afectados

- Microsoft Outlook Express
- Microsoft Windows Mail
- Microsoft Windows Live Mail
- Microsoft Office
- Microsoft Visual Basic for Applications
- Software desarrollado por terceros que usen Visual Basic for Applications

II. Descripción

Microsoft ha liberado boletines de seguridad sobre múltiples vulnerabilidades en Microsoft Outlook Express, Microsoft Windows Mail, Microsoft Windows Live Mail, Microsoft Office, and Microsoft Visual Basic for Applications.

Estos boletines se describen en el Compendio de Boletines de Seguridad Microsoft de Mayo 2010.

Tqmbién se verá afectado el software desarrollado por terceros que usen Visual Basic for Applications que distribuya VBE6.DLL. Si la aplicación sigue las recomedaciones de mejores prácticas para components compartidos como un ensamble punto a punto, el componente puede ser actualizado usando el parche descrito en el boletín MS10-031; de no ser así, se debe contactar al fabricante para conseguir la versión actualizada de la aplicación que contenga el archivo VBE6.DLL actualizado.

III. Impacto

Un usuario remoto no autenticado podría ejecutar código arbitrario o causar que una aplicación vulnerable deje de funcionar.

IV. Solución

Aplique las actualizaciones Microsoft.

Microsoft ha liberado actualizaciones para estas vulnerabilidades en el Compendio de Boletines de Seguridad Microsoft de Mayo 2010. Los boletines describen los problemas conocidos relacionados con las actualizaciones.

Se recomienda a los administradores tomar en cuenta estos problemas y realizar pruebas sobre cualquier efecto adverso. Así mismo deberían de considerar usar un sistema de distribución automática de actualizaciones como Windows Server Update Services (WSUS).

V. Referencias

- Microsoft Security Bulletin Summary for May 2010
- Microsoft Security Bulletin MS10-031 - Critical
- Microsoft Windows Server Update Services

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

- Manuel Ignacio Quintero Martínez (mquintero at seguridad dot unam dot mx)
- Ruben Aquino Luna (raquino at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Cómputo
incidentes at seguridad.unam.mx
phishing at 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 47