UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−002

Vulnerabilidades en Microsoft Windows, Outlook, y Exchange

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades críticas en Windows, Outlook y Exchange. 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:	10 de Enero de 2006
Ultima Revisión:	10 de Enero de 2006
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión.

Sistemas Afectados

Microsoft Windows **Exchange** <KB902412
Microsoft Windows **Outlook** <KB902412
Microsoft Windows
todas las versiones

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Descripción

Los Boletines de Seguridad de Microsoft para Enero de 2006 solucionan vulnerabilidades en Microsoft Windows, Outlook y Exchange. Mayor información está disponible en las siguientes Notas de Vulnerabilidad del US−CERT:

- **VU#915930 − Buffer overflow en las fuentes de Web incrustadas de Microsoft**

  Un buffer overflow basado en heap en la forma en como Microsoft Windows procesa fuentes de Web incrustadas podría permitir a un intruso remoto no autenticado ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−0010)

- **VU#252146 − Vulnerabilidad de decodificación de TNEF en Microsoft Outlook y Microsoft Exchange**

  Microsoft Outlook y Microsoft Exchange contienen una vulnerabilidad no especificada en el procesamiento de archivos adjuntos TNEF. Esto podría permitir a un intruso remoto no autenticado ejecutar código arbitrario en un sistema ejecutando el software vulnerable.
  (CVE−2006−0002)

II. Impacto

La explotación de estas vulnerabilidades podría permitir a un intruso remoto no autenticado ejecutar código arbitrario con los privilegios del usuario. Si el usuario ha iniciado sesión con privilegios administrativos, el intruso podría tomar el control completo de un sistema afectado. Un intruso podría también ser capaz de causar una negación de servicio.

III. Solución

- **Aplicar las actualizaciones**

  Microsoft ha proporcionado las actualizaciones para estas vulnerabilidades en los Boletines de Seguridad y en el sitio Microsoft Update.

- **Soluciones temporales**

  Consulte las Notas de Vulnerabilidades del US−CERT para obtener soluciones temporales a estos problemas.

IV. Apéndice

- Proyecto Seguridad en Windows, DSC/UNAM−CERT − http://www.seguridad.unam.mx/windows
- Resumen de Boletines de Seguridad de Microsoft para Enero de 2006 − <http://www.microsoft.com/technet/security/bulletin/ms06−jan.mspx>
- Nota de Vulnerabilidad del US−CERT VU#915930 − <http://www.kb.cert.org/vuls/id/915930>

- Nota de Vulnerabilidad del US−CERT VU#252146 − <http://www.kb.cert.org/vuls/id/252146>
- CVE−2006−0002 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0002>
- CAN−2006−0010 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0010>
- 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:

- 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