***UNAM−CERT***

***Departamento de Seguridad en Cómputo***

***DGSCA−UNAM***

---

***Boletin de Seguridad UNAM−CERT−2006−019***

***Vulnerabilidad en Microsoft Word***

---

Una vulnerabilidad de buffer overflow en Microsoft Word podría permitir a un intruso ejecutar código arbitrario en un sistema vulnerable.

| | |
|---|---|
| **Fecha de Liberación**: | 19 de Mayo de 2006 |
| **Ultima Revisión**: | 19 de Mayo de 2006 |
| **Fuente**: | CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión. |

**Riesgo**

Crítico

**Problema de Vulnerabilidad**

Local

**Tipo de Vulnerabilidad**

Buffer Overflow

## I. Sistemas afectados

- Microsoft Word 2003
- Microsoft Word XP (2002)

Microsoft Word esta incluido en la Suite de Microsoft Works y Microsoft Office. Otras versiones de Word, y otros programas de Office podrían ser afectados o actuar como vectores de ataque.

## II. Descripción

Microsoft Word contiene una vulnerabilidad de buffer overflow. Abriendo un documento de Word creado de forma maliciosa, incluyendo documentos almacenados en sitios Web o adjuntos a mensajes de correo electrónico, podrían activar la vulnerabilidad.

Los documentos de Office pueden contener objetos incrustados. Por ejemplo, un documento de Word malicioso podría ser incrustado en un documento de Excel y PowerPoint. Los documentos de Office distintos a Word podrían ser utilizados como vectores de ataque.

Para mayor información, consulte la Nota de Vulnerabilidad VU#446012.

## III. Impacto

Convenciendo a un usuario a que abra un documento de Word creado de forma maliciosa, un intruso podría ejecutar código arbitrario en un sistema vulnerable. Si el usuario tiene privilegios administrativos, el intruso podría tomar el control completo del sistema.

## IV. Solución

Al tiempo de escribir este documento, no existe una solución completa disponible. Considere las siguientes soluciones temporales:

- No abrir documentos de Word no confiables.

  No abra documentos de Word u Office poco familiares, incluyendo aquellos recibidos como archivos adjuntos en correos electrónicos o alojados en un sitio Web. Consulte el Tip de Seguridad Cibernética ST04−010 para mayor información.

- No confíe en el filtro de extensiones de archivo.

  En la mayoría de los casos, Windows llama a Word para abrir un documento aún si el documento tiene una extensión de archivo desconocida. Por ejemplo, si *documento.d0c* (note el dígito “0”) contiene el la información de encabezado de archivo correcto, Windows abrirá el documento *documento.d0c* con Word.

## V. Apéndice A. Referencias

- Nota de Vulnerabilidad VU#446012 − <http://www.kb.cert.org/vuls/id/446012>
- Tip de Seguridad Cibernética ST04−010 − <http://www.us−cert.gov/cas/tips/ST04−010.html>

---

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***