UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−022

Vulnerabilidad en Microsoft Excel

Una vulnerabilidad no especificada en Microsoft Excel podría permitir a un intruso ejecutar código arbitrario en un sistema vulnerable.

Fecha de Liberación:	16 de Junio de 2006
Ultima Revisión:	16 de Junio 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

Remoto

Tipo de Vulnerabilidad

Ejecución Remota de Código

I. Sistemas afectados

- Microsoft Excel 2003
- Microsoft Excel XP (2002)
- Microsoft Excel for Mac

Microsoft Excel está incluido con Microsoft Office. Otras versiones de Excel y otros programas de Office podrían ser afectados o actuar como vectores de ataque.

II. Descripción

Microsoft Excel contiene una vulnerabilidad no especificada. Abriendo un documento de Excel creado de forma específica, incluyendo documentos almacenados en sitios Web o adjuntos en mensajes de correo electrónico, podrían activar la vulnerabilidad.

Los documentos de Office pueden contener objetos incrustados. Por ejemplo, un documento de Excel maliciosos podría ser incrustado en un documento de Word o PowerPoint. Los documentos de office diferentes a los de Excel podrían ser utilizados como vectores de ataque.

Para mayor información, consulte la Nota de Vulnerabilidad VU#802324.

III. Impacto

Convenciendo a un usuario de que abra un documento de Excel creado especialmente, un intruso podría ejecutar código arbitrario en un sistema vulnerable. Si un usuario tiene privilegios administrativos, el intruso podría obtener control completo del sistema.

IV. Solución

Al tiempo de la liberación de éste boletín, no existe una solución completa disponible. Considere las siguientes soluciones temporales:

- **No abra documentos de Excel no confiables.**

  No abra documentos de Excel o de Office no familiares o inesperados, incluyendo aquellos que reciba a través de archivos adjuntos de correo electrónico o almacenados 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 llamará a Excel para abrir un documento aún si el documento tiene una extensión de archivo desconocida. Por ejemplo, si el documento .x1s (note el dígito "1") contiene la información de cabecera de archivo correcta, Windows abrirá el documento .x1s con Excel.

V. Apéndice

- Nota de Vulnerabilidad VU#802324 − <http://www.kb.cert.org/vuls/id/802324>
- 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