UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−010

Vulnerabilidades en Microsoft Office y Excel

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades críticas en Microsoft Office y Excel. 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: 14 de Marzo de 2006

Fuente: CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión

Sistemas Afectados

Microsoft Office	==	Microsoft Office 2000 Service Pack 3
Microsoft Office	==	Microsoft Office 2003 Service Pack 1 o Service Pack 2
Microsoft Office	==	Microsoft Office XP Service Pack 3
Microsoft Office	==	Microsoft Works Suites 2000 a

2006

Mac OS X	**Microsoft Office**	==	Microsoft Office 2004 para Mac
Mac OS X	**Microsoft Office**	==	Microsoft Office X para Mac

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Ejecución Remota de Código

I. **Descripción**

El Resumen de Boletines de Seguridad de Microsoft para Marzo de2006 cubre vulnerabilidades en Microsoft Office y Excel. Información adicional está disponible en las siguientes Notas de Vulnerabilidades del US−CERT:

- **VU#339878 − Vulnerabilidad de corrupción de memoria al analizar formatos de archivos malformados en Microsoft Excel**

  Microsoft Excel contiene una vulnerabilidad de corrupción de memoria. Esta vulnerabilidad podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−0028)

- **VU#104302 − Vulnerabilidad de corrupción de memoria en registro malformado en Microsoft Excel**

  Microsoft Excel falla al validar adecuadamente registros. Esta vulnerabilidad podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−0031)

- **VU#123222 − Vulnerabilidad de corrupción de memoria en gráficos malformados en Microsoft Excel**

  Microsoft Excel falla al validar gráficos. Esta vulnerabilidad podría permitir a un intruso remoto ejecutar código arbitrario en el sistema vulnerable.
  (CVE−2006−0030)

- **VU#235774 − Vulnerabilidad de corrupción de memoria en descripción malformada en Microsoft Excel**

Microsoft Excel falla al validar adecuadamente el campo de descripción. Esta vulnerabilidad podría permitir a un intruso remoto ejecutar código arbitrario en el sistema vulnerable.
(CVE−2006−0029)

- **VU#642428 − Microsoft Excel falla al realizar adecuadamente la validación del rango cuando analiza archivos.**

  Microsoft Excel contiene un error en el rango de validación, lo cual podría permitir a un intruso remoto no autenticado ejecutar código arbitrario en un sistema vulnerable
  (CVE−2005−4131)

- **VU#682820 − Buffer overflow en slip de ruteo de Microsoft Office**

  Microsoft Office contiene un buffer overflow en el analizador de slips de ruteo que podría permitir a un intruso ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−0009)

II. Impacto

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

III. Solución

- **Aplicar actualizaciones**

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

- **Soluciones temporales**

  Consulte las siguientes Notas de Vulnerabilidades para obtener soluciones temporales.

IV. Apéndice A. Referencias

- Proyecto Seguridad en Windows, DSC/UNAM−CERT − <http://www.seguridad.unam.mx/windows>
- Resumen de Boletines de Seguridad de Microsoft para Marzote 2006 − <http://www.microsoft.com/technet/security/bulletin/ms06−mar.mspx>
- Nota de Vulnerabilidad del US−CERT VU#339878 − <http://www.kb.cert.org/vuls/id/339878>
- Nota de Vulnerabilidad del US−CERT VU#104302 − <http://www.kb.cert.org/vuls/id/104302>
- Nota de Vulnerabilidad del US−CERT VU#123222 − <http://www.kb.cert.org/vuls/id/123222>
- Nota de Vulnerabilidad del US−CERT VU#235774 − <http://www.kb.cert.org/vuls/id/235774>

- Nota de Vulnerabilidad del US−CERT VU#642428 − <http://www.kb.cert.org/vuls/id/642428>
- Nota de Vulnerabilidad del US−CERT VU#682820 − <http://www.kb.cert.org/vuls/id/682820>
- CVE−2005−4131 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2005−4131>
- CVE−2006−0009 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0009>
- CVE−2006−0028 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0028>
- CVE−2006−0029 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0029>
- CVE−2006−0030 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0030>
- CVE−2006−0031 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0031>
- 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:

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