UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2005−010

Vulnerabilidades en Windows, Internet Explorer y Word

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades críticas en Windows, Office e Internet Explorer. La explotación de estas vulnerabilidades podría permitir a un intruso remoto no autenticado ejecutar código arbitrario en un sistema afectado.

Fecha de Liberación: 12 de Julio de 2005

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

Sistemas Afectados

Microsoft Office	⊲KB903672
Internet Explorer	⊲KB903235
Color Management Module	⊲KB901214

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Ejecución Remota de Código

I. Descripción

Los Boletines de Seguridad de Microsoft para Junio de 2005 solucionan vulnerabilidades en Windows, Office e Internet Explorer. Información adicional está disponible en las siguientes Notas de Vulnerabilidades:

- **VU#218621 − Buffer overflow en la rutina de procesamiento de fuente de Microsoft Word**

  Existe un buffer overflow en la rutina de procesamiento de fuente de Microsoft Word que podría permitir a un intruso remoto ejecutar código en un sistema vulnerable.
  (CAN−2005−0564)

- **VU#720742 − Buffer overflow en Microsoft Color Management Module durante la validación de la etiqueta de perfil**

  Microsoft Color Management Module falla al validar adecuadamente datos de entrada, permitiendo a un intruso remoto ejecutar código arbitrario.
  (CAN−2005−1219)

- **VU#939605 −El objeto COM JVIEW Profiler (javaprxy.dll) contiene una vulnerabilidad no especificada**

  El objeto COM JVIEW Profiler contiene una vulnerabilidad no especificada, la cual podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable.
  (CAN−2005−2087)

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 del sistema afectado.

III. Solución

- **Aplicar actualizaciones**

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

- **Soluciones temporales**

  Consulte las Notas de Vulnerabilidades individuales para obtener soluciones temporales.

IV. Apéndices

- Resumen de Boletines de Seguridad de Microsoft Julio, 2005 − <http://www.microsoft.com/technet/security/bulletin/ms05−jul.mspx>
- UNAM−CERT: Proyecto Seguridad en Windows − <http://www.seguridad.unam.mx/windows/>
- Nota de Vulnerabilidad del US−CERT VU#218621 − <http://www.kb.cert.org/vuls/id/218621>
- Nota de Vulnerabilidad del US−CERT VU#720742 − <http://www.kb.cert.org/vuls/id/720742>
- Nota de Vulnerabilidad del US−CERT VU#939605 − <http://www.kb.cert.org/vuls/id/939605>

- CAN−2005−0564 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−0564>
- CAN−2005−1219 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1219>
- CAN−2005−2087 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−2087>
- Microsoft Update − <http://update.microsoft.com/>
- Introducción a Microsoft Update − <http://www.microsoft.com/technet/prodtechnol/microsoftupdate/default.mspx>

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