UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2005−011

Vulnerabilidades en Microsoft Windows e Internet Explorer

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades críticas en Windows e Internet Explorer. La explotación de estas vulnerabilidades podría permitir a un intruso remoto no autenticado ejecutar código arbitrario o causar una negación de servicio en el sistema afectado.

Fecha de Liberación: 9 de Agosto de 2005

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

Sistemas Afectados

	Internet Explorer	<KB896727
Microsoft Windows todas las versiones	**Servicio de Cola de impresión.**	<KB896423
Microsoft Windows todas las versiones	**Plug and Play**	<KB899588
Microsoft Windows todas las versiones	**Telephony Application Programming Interface**	<KB893756
Microsoft Windows todas las versiones	**Kerberos**	<KB899587
Microsoft Windows todas las versiones	**Remote Desktop Protocol**	<KB899591

Riesgo

Importante

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Descripción

Los Boletines de Seguridad de Microsoft para Agosto de 2005 solucionan vulnerabilidades en Windows e Internet Explorer. Más información está disponible en las siguientes Notas de Vulnerabilidad:

- **VU#965206 − Biblioteca de interpretación de JPEG en Microsoft Internet Explorer es vulnerable a un buffer overflow.**

  Microsoft Internet Explorer contiene un falla relacionada a la interpretación de imágenes JPEGs que podría permitir que un intruso ejecute código arbitrario de forma remota.
  (CAN−2005−1988)

- **VU#959049 − Varios objetos COM causan una corrupción de memoria en Internet Explorer**

  Microsoft Internet Explorer permite la ejemplificación de objetos COM no Active−X, lo cual podría permitir a un intruso ejecutar código arbitrario o causar que falle Internet Explorer.
  (CAN−2005−1990)

- **VU#998653 − Microsoft Plug and Play contiene una vulnerabilidad de buffer overflow**

  Microsoft Plug and Play contiene una falla en el manejo de buffers de mensajes que podría resultar en una condición de negación de servicio y ejecución de código de forma local o remota.
  (CAN−2005−1983)

- **VU#490628 − El servicio Microsoft Remote Desktop Protocol contiene una vulnerabilidad no especificada.**

  Un error de validación de entrada en el servicio Microsoft Remote Desktop Protocol (RDP) podría permitir a un intruso remoto causar una condición de negación de servicio.
  (CAN−2005−1218)

- **VU#220821 − El servicio Microsoft Print Spooler contiene un buffer overflow**

  Un buffer overflow en el servicio Microsoft Print Spooler podría permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable.
  (CAN−2005−1984)

II. Impacto

La explotación de estas vulnerabilidades podría permitir a un intruso remoto no autenticado ejecutar código arbitrario con privilegios de SYSTEM o 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 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 Notas de Vulnerabilidad para aplicar soluciones temporales.

IV. Apéndice

- Proyecto Seguridad en Windows, DSC/UNAM−CERT − <http://www.seguridad.unam.mx/windows>
- Resúmen de Boletines de Seguridad para Agosto, 2005 − <http://www.microsoft.com/technet/security/bulletin/ms05−aug.mspx>
- Nota de Vulnerabilidad del US−CERT VU#965206 − <http://www.kb.cert.org/vuls/id/965206>
- Nota de Vulnerabilidad del US−CERT VU#959049 − <http://www.kb.cert.org/vuls/id/959049>
- Nota de Vulnerabilidad del US−CERT VU#998653 − <http://www.kb.cert.org/vuls/id/998653>
- Nota de Vulnerabilidad del US−CERT VU#490628 − <http://www.kb.cert.org/vuls/id/490628>
- Nota de Vulnerabilidad del US−CERT VU#220821 − <http://www.kb.cert.org/vuls/id/220821>
- CAN−2005−1988 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1988>
- CAN−2005−1990 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1990>
- CAN−2005−1983 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1983>
- CAN−2005−1218 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1218>
- CAN−2005−1984 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1984>
- Microsoft Update − <https://update.microsoft.com/microsoftupdate>
- 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