UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2005−008

Vulnerabilidades en Microsoft Windows e Internet Explorer

Microsoft ha liberado actualizaciones críticas en Windows e Internet Explorer. La explotación de estas vulnerabilidades podría permitir a un intruso no autentificado ejecutar código de forma remota o causar una negación de servicio.

Fecha de Liberación: 15 de Junio de 2005

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

I. Sistemas Afectados

- Microsoft Windows
- Microsoft Internet Explorer

II. Descripción

Los Boletines de Seguridad de Microsoft para Junio de 2005 apuntan a un número de vulnerabilidades en Windows, Internet Explorer, Outlook Express, Outlook Web Access, ISA Server, el motor Step−by−Step Interactive Training y telnet. Más información acerca de estas vulnerabilidades esta disponible en las siguientes notas:

- **VU#189754 − Buffer overflow en la interpretación de imágenes PNG de Microsoft Internet Explorer.**

  Un buffer overflow en el componente de interpretación de imágenes PNG de Microsoft Internet Explorer podría permitir a un intruso ejecutar código en el sistema vulnerable. (CAN−2005−1211)

- **VU#489397 − Microsoft Server Message Block vulnerable a buffer overflow.**

  Microsoft Server Message Block (SMB) es vulnerable a una falla en el manejo de buffer cuando procesa paquetes de entrada lo cual puede

permitir la ejecución de código remota. (CAN−2005−1206)

- **VU#851869 − Error de validación de entrada en la Ayuda HTML de Microsoft.**

  La Ayuda HTML de Microsoft falla al validar apropiadamente la entrada de datos, permitiendo a un intruso ejecutar código arbitrario. (CAN−2005−1208)

III. Impacto

La explotación de la más seria de estas vulnerabilidades podría permitir a un intruso no autentificado ejecutar código arbitrario con privilegios de SYSTEM. Esto podría permitir a un intruso tomar el control total del sistema vulnerable. Un intruso podría también ejecutar código arbitrario con privilegios del usuario, o causar una negación de servicio.

IV. Soluciones

Aplicar las actualizaciones. Microsoft ha proporcionado actualizaciones para estas vulnerabilidades en:

- Boletines de Seguridad
- Windows Update

V. Apéndices

- Seguridad en Windows DSC/UNAM−CERT: Boletines de Seguridad de Microsoft – http://www.seguridad.unam.mx/windows
- Resumen de Boletines de Seguridad de Microsoft para Junio de 2005 – http://www.microsoft.com/technet/security/bulletin/ms05−jun.msp
- Nota de Vulnerabilidad del US−CERT VU#189754 – http://www.kb.cert.org/vuls/id/189754
- Nota de Vulnerabilidad del US−CERT VU#489397 – http://www.kb.cert.org/vuls/id/489397
- Nota de Vulnerabilidad del US−CERT VU#851869 – http://www.kb.cert.org/vuls/id/851869
- CAN−2005−1211 – http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1222
- CAN−2005−1206 – http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1206
- CAN−2005−1208 – http://cve.mitre.org/cgi−bin/cvename.cgi?name=CAN−2005−1208
- Microsoft Windows Update – http://windowsupdate.microsoft.com/

El Departamento de Seguridad en Cómputo/UNAM−CERT agradece el apoyo en la traducción, elaboración y revisión de éste Documento a:

- Juan Lopez Morales (jlopez@correo.seguridad.unam.mx)

- Jesús Ramón Jimenez Rójas (jrojas@seguridad.unam.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