UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2007−029

Actualizaciones de Microsoft para múltiples vulnerabilidades

Microsoft ha liberado actualizaciones que solucionan vulnerabilidades críticas en Microsoft Windows y Microsoft Windows DNS Server. La explotación de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar comandos de su elección o causar que un servidor DNS de Windows proporcione repuestas DNS incorrectas.

Fecha de Liberación: 13 de Noviembre de 2007

Ultima Revisión: 13 de Noviembre de 2007

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

Múltiples vulnerabilidades

I. Sistemas afectados

- Microsoft Windows
- Microsoft Windows DNS Server

II. Descripción

Microsoft ha liberado actualizaciones para solucionar vulnerabilidades que afectan Microsoft Windows y Microsoft Windows DNS Server como parte del Resumen de Boletines de Seguridad de Microsoft para Noviembre de 2007. La más severa de las vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar comandos de su elección o causar que un servidor Windows DNS Server proporcionar respuestas DNS incorrectas.

Mayor información sobre las vulnerabilidades solucionados por estas actualizaciones está disponible en la Base de Datos de Notas de Vulnerabilidades.

III. Impacto

Un atacante remoto no autenticado podría ejecutar comandos arbitrarios en un sistema vulnerable. Un atacante podría ser capaz de causar que un servidor DNS de Windows proporcionar respuestas incorrectas a consultas DNS.

IV. Solución

- **Aplicar actualizaciones de Microsoft**

  Microsoft ha proporcionado actualizaciones para estas vulnerabilidades en los de Noviembre de 2007. Los boletines de seguridad describen cualquier problema conocido relacionado a las actualizaciones. Se recomienda a los administradores notar cualquier problema conocido descrito en los Boletines y probar cualquier afectación potencialmente adversa en su ambiente.

  Los administradores de sistemas podrían desear utilizar un sistema de distribución automatizado de actualizaciones como WSUS (Windows Server Update Services).

V. Referencias

- Proyecto Seguridad en Windows, DSC/UNAM−CERT − <http://www.seguridad.unam.mx/windows>
- Notas de vulnerabilidades del US−CERT para actualizaciones de Microsoft de Noviembre de 2007 − <http://www.kb.cert.org/vuls/byid?searchview&query=ms07−nov>
- Resumen de Boletines de Seguridad de Microsoft de Noviembre de 2007 − <http://www.microsoft.com/technet/security/bulletin/ms07−nov.mspx>
- Microsoft Update − <https://update.microsoft.com/microsoftupdate/>
- Windows Server Update Services − <http://www.microsoft.com/windowsserversystem/updateservices/default.mspx>
- Asegurando tu navegador Web − <http://www.cert.org/tech_tips/securing_browser/>

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
incidentes at seguridad.unam.mx
phishing at 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