

UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA-UNAM

Boletín de Seguridad UNAM-CERT-2008-024

Vulnerabilidad en el servicio Server de Microsoft podría permitir la ejecución remota de código

Microsoft ha liberado actualizaciones para sus sistemas operativos Microsoft Windows fuera del periodo ordinario de actualizaciones debido al reporte de una vulnerabilidad en el servicio Server que podría permitir la ejecución remota de código. Por lo que se sugiere instalar la actualización a la brevedad en sistemas de misión crítica.

Fecha de Liberación: 23 de Octubre de 2008

Última Revisión: 23 de Octubre de 2008

Fuente: Microsoft Corp., Foros y listas de discusión.

I. Índice de Explotación

- ◆ CVE-2008-4250 – Probable existencia de exploit consistente

II. Sistemas Afectados

- ◆ Microsoft Windows 2000
- ◆ Microsoft Windows XP
- ◆ Microsoft Windows Server 2003
- ◆ Microsoft Windows Vista
- ◆ Microsoft Windows Server 2008

III. Descripción

Microsoft ha liberado actualizaciones para sus sistemas operativos Microsoft Windows fuera del periodo ordinario de actualizaciones. La actualización liberada el día de hoy ([Vulnerabilidad en el servicio Server podría permitir la ejecución remota de código \(958644\)](#)) podría permitir a un atacante la ejecución remota de código a través de peticiones RPC en los sistemas operativos Windows 2000, Windows XP y Windows 2003. En los sistemas Windows Vista y Windows Server 2008 la vulnerabilidad podría ocasionar una negación de servicio si el sistema de Prevención de Ejecución de Datos (DEP) está habilitado.

De acuerdo al [boletín oficial de Microsoft](#) existe probabilidad de crear un código exploit que sea consistente y que además podría tener características de

gusano. Por lo que es importante que los administradores tomen las precauciones pertinentes.

IV. Impacto

Un atacante remoto no autenticado podría ejecutar código en el sistema afectado a través del envío de peticiones RPC construidas malintencionadamente. Además de ello los atacantes podrían aprovechar la vulnerabilidad para crear un exploit en forma de gusano.

V. Solución

- ◆ Aplicar actualizaciones de Microsoft Corp.

Microsoft ha proporcionado actualizaciones a través del boletín de seguridad MS08-067, donde se describe cualquier problema conocido y relacionado con las actualizaciones. Se recomienda a los administradores actualizar sus sistemas probando el efecto de las actualizaciones previo a actualizar sus sistemas de producción y así determinar cualquier efecto adverso.

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

VI. Referencias

- ◆ Proyecto Seguridad en Windows, DSC/UNAM-CERT – <http://www.seguridad.unam.mx/windows>
- ◆ Vulnerabilidad en el Servidor de Servicios podría permitir la ejecución remota de código (958644) – <http://www.seguridad.unam.mx/vulnerabilidadesDB/?vulne=5666>
- ◆ Boletín de Seguridad de Microsoft MS08-067 – <http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>
- ◆ Índice de Explotación – <http://www.seguridad.unam.mx/doc/?ap=articulo>
- ◆ CVE-2008-4250 – <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250>
- ◆ Microsoft Update – <https://www.update.microsoft.com/microsoftupdate/>
- ◆ Windows Server Update Services – [http://technet.microsoft.com/es-es/wsus/default\(en-us\).aspx](http://technet.microsoft.com/es-es/wsus/default(en-us).aspx)

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

- Oscar Raúl Ortega Pacheco (oortega at seguridad dot unam dot mx)
- Juan Carlos Guel Lopez (cguel 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

UNAM-CERT

<http://www.cert.org.mx>

<http://www.seguridad.unam.mx>

<ftp://ftp.seguridad.unam.mx>

Tel: 56 22 81 69

Fax: 56 22 80 47