

UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA-UNAM

Nota de Seguridad UNAM-CERT-2008-004

Importante actualizar Sistemas Operativos Windows

En los últimos días UNAM-CERT ha recibido diversos reportes que alertan sobre la aparición de un gusano que explota una vulnerabilidad en los sistemas operativos Windows. UNAM-CERT recomienda a usuarios y administradores de sistemas operativos Windows instalar a la brevedad la actualización de seguridad KB 958644 (MS08-067).

Fecha de Liberación: 1 de Diciembre de 2008

Última Revisión: 1 de Diciembre de 2008

Fuente: Microsoft Corp., foros y listas privadas de discusión.

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

I. Sistemas Afectados

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

II. Descripción

El pasado 23 de octubre Microsoft Corp., liberó una actualización de seguridad de emergencia (MS-067). Dicha actualización soluciona una vulnerabilidad que ha sido clasificada como crítica y que podría permitir a los atacantes tomar control total del sistema afectado. Además, UNAM-CERT ha recibido reportes que muestran la propagación de software malicioso ([Win32/Conficker.A](#), [Win32/IRCbot.BH](#)) que está explotando exitosamente la vulnerabilidad. La vulnerabilidad se encuentra en el servicio Server de Microsoft y podría explotarse enviando solicitudes maliciosas de RPC por lo que es importante que

UNAM-CERT

los usuarios actualicen sus sistemas operativos Windows.

Para mayores informes sobre la vulnerabilidad visite el siguiente boletín:

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

III. Impacto

Se ha identificado la propagación de software maliciosos que está explotando la vulnerabilidad MS08-067 para comprometer equipos con sistemas operativos Windows y tomar control total de los sistemas afectados.

IV. Solución

El UNAM-CERT recomienda a los usuarios aplicar una actualización de seguridad de Microsoft Corp.

- ◆ Microsoft Windows 2000 Service Pack 4
- ◆ Windows XP Service Pack 2 y Windows XP Service Pack 3
- ◆ Windows XP Professional x64 Edition y Windows XP Professional x64 Edition Service Pack 2
- ◆ Windows Server 2003 Service Pack 1 y Windows Server 2003 Service Pack 2
- ◆ Windows Server 2003 x64 Edition y Windows Server 2003 x64 Edition Service Pack 2
- ◆ Windows Server 2003 con SP1 para sistemas basados en Itanium y Windows Server 2003 con SP2 para sistemas basados en Itanium
- ◆ Windows Vista y Windows Vista Service Pack 1
- ◆ Windows Vista x64 Edition y Windows Vista x64 Edition Service Pack 1
- ◆ Windows Server 2008 para sistemas de 32-bits *
- ◆ Windows Server 2008 para sistemas x64 *
- ◆ Windows Server 2008 para sistemas basados en Itanium

* Nota: Los sistemas instalados en modo Server Core también son afectados por lo que deberán instalar la actualización de seguridad.

Otras medidas para prevenir o erradicar la infección podrían ser las siguientes:

- ◆ Instalar y actualizar un sistema antivirus y posteriormente realizar un análisis completo del sistema.
- ◆ Realizar un análisis en línea del sistema operativo (Windows Live OneCare Examen de Seguridad).
- ◆ Activar el Firewall
- ◆ No abrir archivos o correos de remitentes desconocidos.

V. Referencias

- ◆ Microsoft hace un llamado a los usuarios de PC para que instalen actualización de seguridad – <http://www.microsoft.com/latam/prensa/2008/noviembre/alerta.aspx>
- ◆ Vulnerabilidad en el servicio Server de Microsoft podría permitir la ejecución remota de código –

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)
 - Ruben Aquino Luna (raqino 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 47