UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2008−030

Actualizaciones de Microsoft para múltiples vulnerabilidades

Microsoft ha liberado actualizaciones que solucionan diversas vulnerabilidades en sus productos Microsoft Windows, Microsoft Office, Internet Explorer, Visual Basic y Windows Media.

Fecha de Liberación:	9 de Diciembre de 2008
Ultima Revisión:	9 de Diciembre de 2008
Fuente:	Microsoft Corp. CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como foros y listas de discusión.

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

I. Sistemas Afectados

- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 2003
- Microsoft Windows 2008
- Internet Explorer
- Visual Basic 6
- Microsoft Office
- Microsoft Office Word
- Microsoft Office Excel
- Microsoft Office SharePoint Server
- Windows Media

II. Descripción

Microsoft ha liberado actualizaciones para solucionar vulnerabilidades que afectan algunos servicios y aplicaciones en sus sistemas operativos Windows 2000, Windows XP, Windows Server 2003, Windows Vista y Windows Server 2008 como parte del Resumen de Boletines de Seguridad del mes de diciembre de 2008. El resumen contiene la descripción de seis boletines clasificados como críticos y dos boletines clasificados como importantes por lo que se recomienda a los administradores de sistemas Windows tomar las precauciones pertinentes.

III. Impacto

La más severa de las vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario y tomar control total del sistema afectado.

IV. Solución

- Aplicar actualizaciones de Microsoft Corp.

  Microsoft ha proporcionado actualizaciones para estas vulnerabilidades en sus boletines de seguridad del mes de diciembre de 2008. Los boletines de seguridad describen 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).

V. Observaciones

A partir de los boletines de seguridad correspondientes al mes del octubre Microsoft proporciona información acerca de la disponibilidad del código que explote la vulnerabilidad descrita en la sección Índice de Explotación.

Si desea conocer mayor información acerca de éste índice visite el siguiente documento:

- Índice de Explotación
  - ◊ http://www.seguridad.unam.mx/doc/?ap=articulo/ul>

VI. Referencias

- Proyecto Seguridad en Windows, DSC/UNAM−CERT − http://www.seguridad.unam.mx/windows
- Notas de Vulnerabilidad del US−CERT para actualizaciones de Microsoft de diciembre de 2008 − http://www.kb.cert.org/vuls/byid?searchviewa>
- Resumen de Boletines de Seguridad de Microsoft para diciembre de 2008 − http://www.microsoft.com/technet/security/bulletin/ms08−dec.mspx
- Índice de Explotación de Microsoft − http://technet.microsoft.com/en−us/security/cc998259.aspx

- Microsoft Update − https://www.update.microsoft.com/microsoftupdate/
- Windows Server Update Services − http://technet.microsoft.com/es−es/wsus/default(en−us).aspx
- Índice de Explotación − http://www.seguridad.unam.mx/doc/?ap=articulo

---

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)

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