UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2008−032

Vulnerabilidad en Internet Explorer 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 Internet Explorer que podría permitir la ejecución remota de código. Por lo que se sugiere instalar la actualización a la brevedad en sistemas de mision critica.

Fecha de Liberación: 17 de Diciembre de 2008

Ultima Revisión: 17 de Diciembre de 2008

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

I. Índice de Explotación

- CVE−2008−4844 − Probable existencia de exploit consistente

II. Sistemas Afectados

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP (Todas las versiones)
- Microsoft Windows Vista (Todas las versiones)
- Microsoft Windows Server 2003 (Todas las versiones)
- Microsoft Windows Server 2008 (Todas las versiones)

III. Descripción

Microsoft ha liberado actualizaciones para sus sistemas operativos Microsoft Windows fuera del periodo ordinario de actualizaciones (UNAM−CERT−2008−080). Dicha actualización de seguridad soluciona una vulnerabilidad conocida en Internet Explorer que podría permitir a un atacante ejecutar código remoto. Por lo que se sugiere a administradores y usuarios de sistemas Windows actualizar sus equipos a la brevedad posible.

IV. Impacto

Un atacante remoto podría ejecutar código arbitrario y obtener los mismos privilegios que el usuario en sesión.

V. Solución

- Aplicar actualizaciones de Microsoft Corp.

  Microsoft ha proporcionado actualizaciones a través del boletín de seguridad MS08−078, 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
- Actualización de seguridad para Internet Explorer (960714) − http://www.seguridad.unam.mx/vulnerabilidadesDB/?vulne=5689
- Boletín de Seguridad de Microsoft MS08−078 − http://www.microsoft.com/technet/security/Bulletin/MS08−078.mspx
- Índice de Explotación − http://www.seguridad.unam.mx/doc/?ap=articulo
- CVE−2008−4844 − http://www.cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−CVE−2008−4844
- Microsoft Update − https://www.update.microsoft.com/microsoftupdate/
- Windows Server Update Services − 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)

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