UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA-UNAM

Boletin de Seguridad UNAM-CERT-2010-002

Vulnerabilidades en las fuentes de Microsoft Windows EOT y en Adobe Flash Player 6

Microsoft ha liberado actualizaciones para solucionar una vulnerabilidad en el motor de fuentes del Windows Embedded Open Type (EOT). Microsoft ha también publicado una recomendación acerca de múltiples vulnerabilidades en Adobe (Macromedia) Flash Player 6 que está incluido con Windows XP.

Fecha de Liberación: 12 de Enero de 2010

Ultima Revisión: 12 de Enero de 2010

Fuente: National Cyber Alert System

CVE ID: **TA10-012B**

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

I. Sistema Afectado

Microsoft Windows and Internet Explorer

Adobe (Macromedia) Flash Player 6

II. Descripción

El Boletín de Seguridad de Microsoft MS10-001 describe una vulnerabilidad en el motor de fuentes del Embedded Open Type (EOT) de Windows. Microsoft Security Advisory (979267) recomienda que los usuarios de Windows XP remuevan o actualicen Adobe Flash Player 6 (formalmente Macromedia Flash Player) que está incluido en Windows XP. Vulnerability Note VU#204889 discute una vulnerabilidad en Flash Media Player 6 y provee varias soluciones.

Estas vulnerabilidades podrían ser explotadas mediante la carga de fuentes especialmente preparadas o contenido Flash vía Internet Explorer.

Microsoft asigna a la vulnerabilidad de fuentes EOT un grado de severidad bajo en la versiones mas actuales de Windows y señala que la ejecución de código es poco probable. El grado de severidad para Windows 2000, sin embargo, es critico .

III. Impacto

Un atacante remoto, no autenticado, podría ejecutar código arbitrario, obtener privilegios elevados, o causar que una aplicación vulnerable deje de funcionar.

IV. Solución

Aplicar actualizaciones de Microsoft

El Boletín de Seguridad de Microsoft MS10-001 provee actualizaciones para la vulnerabilidad de fuentes del EOT. El boletín de seguridad describe cualquier cuestión conocida relacionada con las actualizaciones. Se les recomienda a los administradores tener en cuenta estos problemas y probar algún potencial efecto adverso. Los administradores deben considerar utilizar un sistema de distribución de actualizaciones automáticas tal como Windows Server Update Services (WSUS).

Actualizar, remover, o deshabilitar Adobe Flash Player 6

Adobe Flash Player 6 está incluido con Windows XP. Adobe ha encarado estas vulnerabilidades en las más nuevas versiones de Flash Player. Actualizar a una versión más reciente de Flash Player (tal como Flash Player 10). De manera alternativa, desinstalar Flash Player o establecer el kill bit para el control del Flash Player ActiveX como es descrito en el Security Advisory (979267) y en el Vulnerability Note VU#204889.

V. Referencias

1. Microsoft Security Bulletin Summary for January 2010
2. Microsoft Security Bulletin MS10-001
3. MS10-001: Font file decompression vulnerability
4. CVE-2010-0018
5. Vulnerabilities in Adobe Flash Player 6 Provided in Windows XP Could Allow Remote Code Execution
6. Vulnerability Note VU#204889
7. Adobe Flash Player
8. How to uninstall the Adobe Flash Player plug-in and ActiveX control
9. Windows Server Update Services (WSUS)

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

- Mayra Villeda (mvilleda at seguridad dot unam dot mx)
- Francisco Carlos Martínez Godínez (fmartinez dot seguridad at gmail dot com)
- Manuel Ignacio Quintero Martínez (mquintero 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