

UNAM-CERT**Departamento de Seguridad en Cómputo****DGSCA-UNAM**

Boletín de Seguridad UNAM-CERT-2008-025

Múltiples Vulnerabilidades en Acrobat y Adobe Reader

Adobe ha liberado el boletín de seguridad APSB08-19 que se refiere a múltiples vulnerabilidades que afectan Adobe Reader y Acrobat. La más grave de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario.

Fecha de Liberación: 4 de Noviembre de 2008

Última Revisión: 6 de Noviembre de 2008

Fuente: CERT/CC

Sistemas Afectados

Microsoft Windows	Adobe Acrobat	<=8.1.2
Microsoft Windows	Adobe Reader	<=8.1.2

Riesgo

Alto

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Descripción

El boletín de seguridad de Adobe [APSB08-19](#) menciona una serie de vulnerabilidades que afectan a la familia de productos de Adobe Acrobat, incluyendo Adobe Reader. Las versiones 8.1.2 y anteriores son vulnerables. Pueden encontrarse más detalles en la [base de datos de vulnerabilidades](#).

Un intruso podría explotar estas vulnerabilidades convenciendo a un usuario de cargar un archivo especialmente creado de Adobe Portable Document (PDF). Acrobat se integra con los navegadores web más populares y visitar un sitio

web suele ser suficiente para causar que Acrobat cargue un contenido PDF.

II. Impacto

Los impactos de estas vulnerabilidades varían. La mas grave de estas vulnerabilidades permite a un atacante remoto ejecutar código arbitrario.

III. Solución

Según la información en el boletín de seguridad de Adobe [APSB08-19](#), los usuarios con la versión 8 de Adobe Reader o Acrobat debería actualizar a la versión 8.1.3.

Deshabilitar la visualización automática en el navegador web de documentos en formato PDF

Prevenir que documentos PDF se abran dentro de un navegador web puede mitigar esta vulnerabilidad. Aplicar las siguientes medidas, además de actualizar, puede prevenir la explotación automática de vulnerabilidades similares.

Para evitar que los documentos PDF se abran automáticamente en un navegador web o con Acrobat Reader:

1. Abrir el Adobe Acrobat o Adobe Reader
2. Abra el menú Edición
3. Elija la opción Preferencias
4. Elige la sección de Internet
5. De-seleccione la opción "Mostrar PDF en el navegador" en la casilla de verificación

Deshabilitar la apertura automática de documentos PDF en Microsoft Internet Explorer.

La desactivación de apertura automática de archivos PDF en Microsoft Internet Explorer (IE) requiere un segundo paso. Para configurar IE para que solicite una confirmación antes de abrir un archivo PDF, deshabilite la opción "Mostrar PDF en el navegador" (como se ha descrito anteriormente) y, a continuación, realice los siguientes cambios en el registro de Windows:

Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\AcroExch.Document.7]

"EditFlags"=hex:00,00,00,00

Desactivar JavaScript en Adobe Reader y Acrobat

La desactivación de Javascript en Adobe Reader y Acrobat puede impedir que esta vulnerabilidad se explote. En Acrobat Reader, JavaScript se puede deshabilitar en el cuadro de diálogo de preferencias General:

1. Abra el menú Edición
2. Elija la opción Preferencias

3. Elija la opción JavaScript
4. De-seleccionar "Habilitar JavaScript Acrobat"

IV. Referencias

- ◆ Adobe Security Bulletin APSB08-19 –
<http://www.adobe.com/support/security/bulletins/apsb08-19.html>
- ◆ US-CERT Vulnerability Notes for Adobe Security Bulletin
APSB08-19 – <http://www.kb.cert.org/vuls/byid?searchview/a>
- ◆ Securing Your Web Browser –
http://www.us-cert.gov/reading_room/securing_browser/

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

- José Roberto Sánchez Soledad (rsanchez at seguridad dot unam dot mx)
- Ruben Aquino Luna (raquino 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