UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2009−013

Vulnerabilidades en Adobe Reader y JavaScript

Adobe ha liberado el boletín de seguridad APSB09−06, el cual describe actualizaciones de Adobe Reader y Acrobat para dos vulnerabilidades de JavaScript que podrían permitir a un atacante remoto la ejecución de código arbitrario.

Fecha de Liberación: 14 de Mayo de 2009

Ultima Revisión: 14 de Mayo de 2009

Fuente:

CVE ID: **CVE−2009−1492**
CVE−2009−1493

Riesgo

Alto

Problema de Vulnerabilidad

Remoto

I. Sistemas Afectados

- Adobe Reader 9.1, 8.1.4, 7.1.1 y anteriores
- Adobe Acrobat Standard, Pro, y Pro Extended versiones 9.1, 8.1.4, 7.1.1 y anteriores

II. Descripción

El boletín de seguridad de Adobe APSB09−06 anuncia actualizaciones para dos vulnerabilidades que afectan a Adobe Reader y Acrobat

- Una vulnerabilidad en el método getAnnots() (CVE−2009−1492) afecta a Adobde Reader y Acrobat para Microsoft Windows, Apple Mac OS X y UNIX.
- Una vulnerabilidad en el método customDictionaryOpen() (CVE−2009−1493) al parecer solo afecta a Adobe Reader para UNIX.

Para mayor información, consulte la nota de vulnerabilidad VU#970180

Un atacante podría explotar estas vulnerabilidades al convencer a un usuario de abrir un archivo Adobe Portable Document Format (PDF) especialmente creado. Acrobat se integra con varios navegadores Web populares y normalmente visitar un sitio Web es suficiente para causar que Reader o Acrobat abran un archivo PDF.

III. Impacto

Al convencer al una víctima de abrir un archivo PDF especialmente creado, un intruso remoto sin necesidad de autenticarse podría ejecutar código arbitrario.

IV. Solución

Actualizar

Adobe ha liberado actualizaciones para remediar este problema. Se recomienda a los usuarios que lean el boletín de seguridad de Adobe APSB09−06 y actualicen las versiones vulnerables de Adobe Reader y Acrobat. De acuerdo a este boletín, estas vulnerabilidades se remedian en las versiones 9.1.1, 8.1.5, y 7.1.2 de Adobe Reader y Acrobat.

Deshabilitar JavaScript en Adobe Reader y Acrobat

Deshabilitar JavaScript previene que estas vulnerabilidades sean explotadas y reduce el riesgo de ataque. Si se hace esto a versiones actualizadas de Adobe Reader y Acrobat, puede proteger de futuras vulnerabilidades.

Para deshabilitar JavaScript en Adobe Reader:

1. Abra Adobe Reader.
2. Abra el menu *Edit*
3. Elija la opción *Preferences...*
4. Elija la sección *JavaScript*
5. Deshabilite la casilla *Enable Acrobat JavaScript*

Deshabilitar JavaScript no resolverá las vulnerabilidades, solo deshabilitará el componente vulnerable de JavaScript. Cuando JavaScript se deshabilita, Adobe Reader y Acrobat preguntarán si se debe rehabilitar JavaScript cuando se abra un PDF que contiene JavaScript.

Prevenir que Internet Explorer abra documentos PDF automáticamente.

El instalador de Adobe Reader y Acrobat configura Internet Explorer para abrir automáticamente archivos PDF sin ninguna interacción del usuario. Este comportamiento puede ser revertido por la opción mas segura que pregunta al usuario importando las siguientes líneas como un archivo .REG:

Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\AcroExch.Document.7]

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

Deshabilitar el despliegue de documentos PDF en el navegador Web

Prevenir que los documentos PDF se abran dentro del navegador Web reduce el riesgo de ser atacado. Si esto se aplica a las versiones actualizadas de Adobe Reader y Acrobat, puede proteger de futuras vulnerabilidades.

Para prevenir que los documentos PDF se abran automáticamente en el navegador Web con Adobe Reader:

1. Abra Adobe Acrobat Reader
2. Abra el menu *Edit*
3. Escoja la opción *Preferences*
4. Escoja la sección *Internet*

Desactive la casilla "*Display PDF in browser*"

Renombrar o eliminar Annots.api

Para deshabilitar el método vulnerable getAnnots(), renombre o elimine el archivo Annots.api. Esto deshabilitara ciertas funciones de Anotaciones, sin embargo las anotaciones aun se pueden visualizar. Esto no protege contra la vulnerabilidad en el método customDictionaryOpen().

En Windows, Annots.api se encuentra normalmente en:

"%ProgramFiles%\Adobe\Reader 9.0\Reader\plug_ins"

En GNU/Linux, por ejemplo, puede estar en:

/opt/Adobe/Reader8/Reader/intellinux/plug_ins/Annots.api

No acceda a documentos PDF de fuentes no confiables

No abra documentos PDF no familiares o inesperados, particularmente aquellos alojados en sitios Web o enviados en archivos adjuntos por correo electrónico.

V. Referencias

- Nota de Vulnerabilidad VU#970180 − http://www.kb.cert.org/vuls/id/970180
- Cyber Security Tip ST04−010: Using Caution with Email Attachments − http://www.us−cert.gov/cas/tips/ST04−010.html
- Adobe Security Bulletin APSB09−06 − http://www.adobe.com/support/security/bulletins/apsb09−06.html
- CVE−2009−1492 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2009−1492
- CVE−2009−1493 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2009−1493

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

- Jesús Mauricio Andrade Guzmán (mandrade 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