

UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA-UNAM

Boletín de Seguridad UNAM-CERT-2010-004

Múltiples Vulnerabilidades en Adobe Reader y Acrobat

Adobe ha publicado el boletín de seguridad APSB10-02, que describe múltiples vulnerabilidades que afectan a Adobe Reader y Acrobat.

Fecha de Liberación: 20 de Enero de 2010

Última Revisión: 21 de Enero de 2010

Fuente: US-CERT

Sistemas Afectados

Multiple Multiple	Adobe Acrobat	< 9.2
Multiple Multiple	Adobe Acrobat	< 9.x

Sistemas No Afectados

Multiple Multiple	Adobe Reader	< 8.1.7
Multiple Multiple	Adobe Reader	< 8.x

Riesgo

Moderado

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Ejecución remota de código y negación de servicio

I. Descripción

Adobe Security Advisory APSB10-02 describe una serie de vulnerabilidades que afectan a Adobe Reader y Acrobat. Estas vulnerabilidades afectan a Adobe Reader 9.2 y versiones anteriores a 9.x, 8.1.7 y versiones anteriores a 8.x. Los

detalles están disponibles en la base de datos de seguridad del US-CERT.

Un atacante podría explotar estas vulnerabilidades persuadiendo a un usuario para que abra un archivo PDF especialmente diseñado. El plug-in de Adobe Reader del navegador está disponible para múltiples navegadores web y sistemas operativos, los cuales pueden abrir automáticamente documentos PDF alojados en una página web.

Algunas de estas vulnerabilidades están siendo explotadas.

II. Impacto

Estas vulnerabilidades podrían permitir a un atacante remoto ejecutar código arbitrario, escribir archivos o carpetas en el sistema de archivos, escalar privilegios, o causar una negación de servicio en un sistema afectado como resultado de abrir un documento PDF malicioso por el usuario.

III. Solución

Actualización

Adobe ha publicado actualizaciones para solucionar este problema. Los usuarios deben leer el boletín de seguridad APSB10-02 y la actualización de versiones vulnerables de Adobe Reader y Acrobat.

Deshabilitar JavaScript en Adobe Reader y Acrobat

Desactivar JavaScript puede impedir que algunos exploits den como resultado la ejecución de código. Acrobat JavaScript puede ser desactivado mediante el menú Preferencias (Editar -> Preferencias -> JavaScript; desmarcar Habilitar Acrobat JavaScript).

Evitar que Internet Explorer abra automáticamente los documentos PDF.

El instalador de Adobe Acrobat Reader y las configuraciones de Internet Explorer pueden abrir automáticamente los archivos PDF sin ningún tipo de interacción del usuario. Este comportamiento puede ser revertido con una opción más segura que le pida al usuario la importación de los siguientes archivos como .REG.

Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\AcroExch.Document.7]

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

Desactivar la visualización de documentos PDF en el navegador web

La prevención de la apertura de documentos PDF dentro de un navegador web mitiga parcialmente esta vulnerabilidad. Si esta solución es aplicada también puede mitigar futuras vulnerabilidades.

UNAM-CERT

Para evitar que los documentos PDF se abran automáticamente en un navegador web, haga lo siguiente:

1. Abrir Adobe Acrobat Reader.
2. Ir a menu Edicion.
3. Elija la opción Preferencias.
4. Elija la sección de Internet.
5. Desmarca la casilla de verificación "Mostrar PDF en el navegador".

No acceder a documentos PDF de fuentes no confiables

No abrir documentos PDF desconocido o inesperado, particularmente los alojados en sitios web o que se envían como archivos adjuntos de correo electrónico. Por favor vea los Consejos de Seguridad Cibernética ST04-010.

IV. Referencias

- * Adobe Security Bulletin APSB10-02 - <http://www.adobe.com/support/security/bulletins/apsb10-02.html>
- * Vulnerability Note VU#508357 - <https://www.kb.cert.org/vuls/id/508357>
- * Vulnerability Note VU#773545 - <https://www.kb.cert.org/vuls/id/773545>

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)

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