

UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA-UNAM

Boletín de Seguridad UNAM-CERT-2010-011

Vulnerabilidades en Adobe Reader y Acrobat

Adobe ha liberado el Boletín de Seguridad APSB10-09, el cual describe múltiples vulnerabilidades que afectan al Adobe Reader y Acrobat.

Fecha de Liberación: 14 de Abril de 2010

Última Revisión: 14 de Abril de 2010

Fuente: US-CERT

Sistemas Afectados

Multiple	Multiple	Adobe Acrobat	<=	8.2.1
Multiple	Multiple	Adobe Acrobat	==	9.3.1
Multiple	Multiple	Adobe Acrobat	<=	9.x
Multiple	Multiple	Adobe Reader	<=	8.2.1
Multiple	Multiple	Adobe Reader	==	9.3.1
Multiple	Multiple	Adobe Reader	<=	9.x

Riesgo

Alto

Problema de Vulnerabilidad

Local y remoto

Tipo de Vulnerabilidad

Ejecución remota de código y Elevación de privilegios

I. Descripción

El Boletín de Seguridad [APSB10-09](#) describe cierto número de vulnerabilidades que afectan a Adobe Reader y Acrobat. Estas vulnerabilidades afectan a Adobe Reader y Acrobat en sus versiones 9.3.1 y versiones anteriores a la 9.x, así como la versión 8.2.1 y anteriores, de los programas mencionados.

Un atacante podría explotar estas vulnerabilidades convenciendo al usuario de abrir un archivo PDF especialmente diseñado. El plug-in para navegador del Adobe Reader, está disponible para múltiples navegadores web así como sistemas operativos y los cuales pueden abrir automáticamente documentos PDF ubicados en un sitio web.

II. Impacto

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

III. Solución

Actualización

Adobe ha liberado actualizaciones para solucionar este problema. Se recomienda a los usuarios leer el Boletín de Seguridad de Adobe [APSB10-09](#) y actualizar las versiones de Adobe Reader y Acrobat.

Adobe no ofrece instaladores independientes para las versiones 9.3.2 y 8.2.2 de Adobe Reader o Acrobat. Para una instalación nueva, primero instalar el Adobe Reader 9.3.0 o 8.2.0 y posteriormente se debe utilizar la característica de actualización automática o instalar la actualización apropiada referenciada en el boletín [APSB10-09](#).

Deshabilitar JavaScript en Adobe Reader y Acrobat

Al deshabilitar JavaScript se puede prevenir que algunos exploits terminen en la ejecución de código. Acrobat JavaScript puede deshabilitarse usando el menú Edición->Preferencias-> JavaScript y deshabilitar la casilla de verificación Habilitar AcrobatJavaScript.

Adobe proporciona un framework para bloquear APIs específicas de JavaScript. Si JavaScript debe estar habilitado, esta característica puede ser útil cuando se sabe que APIs específicas son vulnerables, o usadas en ataques.

Prevenir que Internet Explorer abra automáticamente documentos PDF

El instalador para Adobe Reader y Acrobat configura Internet Explorer para abrir automáticamente archivos PDF sin ninguna interacción del usuario. Este comportamiento puede ser modificado a una opción más segura que pregunte al usuario si lo quiere importar como un archivo .REG, de la siguiente forma:

Editor del Registro de Windows versión 5.00

[HKEY_CLASSES_ROOTAcroExch.Document.7]

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

Deshabilitar la visualización de documentos PDF en el navegador web

UNAM-CERT

Prevenir que los documentos PDF sean abiertos dentro de los navegadores web mitigará parcialmente esta vulnerabilidad. Si esta solución es aplicada, también mitiga futuras vulnerabilidades.

Para prevenir que los documentos PDF sean abiertos automáticamente en el navegador, hacer lo siguiente:

1. Abrir Adobe Acrobat Reader
2. Abrir el menú Edición
3. Escoger la opción preferencias
4. Seleccionar la sección de Internet
5. Deshabilitar la opción Mostrar PDF en el buscador

No acceder a documentos PDF desde fuentes no confiables

No abrir documentos PDF no familiares o inesperados, particularmente aquellos almacenados en sitios web o enviados como archivo adjunto en correos. Por favor, revisar el Tip de Seguridad Cibernética ST04-010.

IV. Referencias

* Actualización de seguridad disponible para Adobe Reader y Acrobat: -
<http://www.adobe.com/support/security/bulletins/apsb10-09.html>

* Próximo por ser liberado Adobe Reader y Acrobat 9.3.2 y 8.2.2 por una nueva actualización: -
<http://www.adobe.com/support/security/bulletins/apsb10-09.html>

* Adobe Reader y Acrobat JavaScript Blacklist Framework -
http://kb2.adobe.com/cps/504/cpsid_50431.html

El Departamento de Seguridad en Computo/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 Computo
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