Subdirección de Seguridad de la Información - UNAM-CERT -- DGSCA-UNAM

Boletin de Seguridad UNAM-CERT-2010-028 Adobe Reader y Acrobat afectadas por múltiples vulnerabilidades

Adobe ha liberado el boletín de seguridad APSB10-21, el cual describe múltiples vulnerabilidades que afectan a Adobe Reader y Acrobat.

- **Fecha de Liberación:** 6-Oct-2010
- **Ultima Revisión:** 6-Oct-2010
- **Fuente:** http://www.us-cert.gov/cas/techalerts/TA10-279A.html
- **Riesgo** Alto
- **Problema de Vulnerabilidad** Local y remoto
- **Tipo de Vulnerabilidad** Ejecución Remota de Código

Sistemas Afectados

Multiple Multiple	Adobe Acrobat	<=	8.2.4
Multiple Multiple	Adobe Acrobat	<=	9.3.4
Multiple Multiple	Adobe Reader	<=	8.2.4
Multiple Multiple	Adobe Reader	<=	9.3.4

1. ## Descripción

   El boletín de seguridad de Adobe APSB10-21 describe una serie de vulnerabilidades que afectan a Adobe Reader y Acrobat. Estas vulnerabilidades afectan a sus productos Reader y Acrobat 9.3.4 y versiones anteriores a 9.x, también a la versión 8.2.4, y versiones anteriores a 8.x.

   Un atacante podría explotar estas vulnerabilidades convenciendo a un usuario que abra un archivo PDF especialmente alterado. El plug-in de Adobe Reader, el cual abre automáticamente archivos PDF situados en sitios web, está disponible para múltiples navegadores y sistemas operativos.

   Información adicional está disponible en la nota del US-CERT VU#491991

2. ## Impacto

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

3. ## Solución

   1) Actualizar

   Adobe ha liberado actualizaciones para corregir estos problemas. Se ha promovido que los usuarios lean el boletín de seguridad de Adobe APSB10-21 y actualizar las versiones vulnerables de Adobe Reader y Acrobat.

   2) Deshabilitar JavaScript en Adobe Reader y Acrobat

Deshabilitando JavaScript podría prevenir algunos exploits resultados de ejecución de código. Acrobat JavaScript puede ser deshabilitado usando el menú preferencias (Edit -> Preferences -> JavaScript; quitar Habilitar Acrobat JavaScript).

Adobe provee un framework para poner en una lista negra APIs específicas de JavaScript. Si JavaScript debe ser habilitado, esta característica puede ser útil cuando se conoce alguna API vulnerable o usada en algún ataque.

3) Prevenir a Internet Explorer de abrir automaticamente archivos PDF

El instalador de Adobe Reader y Acrobat configura a Internet Explorer para abrir automáticamente archivos PDF sin la interacción del usuario. Este comportamiento puede ser revertido importando lo siguiente como un archivo .REG

_____

Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOTAcroExch.Document.7]

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

_____

4) Desactivar el visualizador de archivos PDF en el navegador

Previniendo la apertura de archivos PDF en el navegador, ayudará parcialmente a mitigar esta vulnerabilidad. Si esto es aplicado podría también mitigar vulnerabilidades futuras.

Para prevenir la apertura automática de archivos PDF en el navegador haga lo siguiente:

- Abra Acrobat Reader

- Abra el menú Editar

- Selecciones la opción Preferencias

- Seleccione la sección Internet

- Quite la marca en el checkbox "Mostrar PDF en el navegador"

5) No acceder a archivos PDF de sitios no confiables

No abrir archivos PDF inesperados o que no le parezcan familiares, particularmente en sitios web o como adjuntos en un correo. Por favor ver el tip de seguridad ST04-010.

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

- Javier Santillán Arenas (jsantillan at seguridad dot unam dot mx)
- José Roberto Sánchez Soledad (rsanchez at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Subdirección de Seguridad de la Información

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