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

Boletin de Seguridad UNAM-CERT-2010-020 Vulnerabilidades de Adobe Reader y Adobe Acrobat

Múltiples vulnerabilidades (cf. Adobe Security Bulletin APSB10-17) permiten la ejecución de código arbitrario mediante la lectura de archivos PDF malicios, en diferentes versiones del software, en múltiples sistemas operativos.

- **Fecha de Liberación:** 19-Ago-2010
- **Ultima Revisión:** 20-Ago-2010
- **Fuente:** National Cyber Alert System, US-CERT
- **Riesgo** Muy Alto
- **Problema de Vulnerabilidad** Local y remoto
- **Tipo de Vulnerabilidad** Múltiples vulnerabilidades

Sistemas Afectados

Multiple Multiple	Adobe Acrobat	<=	8.2.3
Multiple Multiple	Adobe Acrobat	<=	9.3.3
Multiple Multiple	Adobe Reader	<=	8.2.3
Multiple Multiple	Adobe Reader	<=	9.3.3

1. ## Descripción

   El boletín de seguridad de Adobe, APSB10-17, describe una cantidad de vulnerabilidades que afectan a Adobe Reader y Adobe Acrobat. Estas vulnerabilidades afectan a Reader y Acrobat 9.3.3, versiones 9.x anteriores, 8.2.3, y versiones 8.x anteriores.

   Un atacante puede explotar estas vulnerabilidades al convencer a un usuario que abra un archivo PDF especialmente diseñado. El plug-in de Adobe Reader para navegadores web, que puede abrir automáticamente documentos PDF almacenados en un sitio web, es también vulnerable, y está disponible para múltiples navegadores web y sistemas operativos.

2. ## Impacto

   Estas vulnerabilidades podrían permitir a un atacante remoto:

   - Ejecutar código arbitrario,

   - Escribir en archivos o carpetas arbitrarias del sistema,

   - Escalar privilegios de sistema,

   - Causar una negación de servicio,

   en sistemas afectados, como resultado de la apertura de un archivo PDF malicioso por parte del usuario.

Solución

Actualización

Adobe ha liberado actualizaciones para corregir estos problemas. Se le sugiere a los usuarios que lean el boletín APSB10-17 de Adobe, y actualicen sus versiones vulnerables de Adobe Reader y Acrobat.

Deshabilitar Javascript en Adobe Reader y Acrobat

Deshabilitar Javascript puede prevenir que algunos exploits resulten en ejecución de código. Javascript puede ser deshabilitado en el software de Acrobat, utilizando el menú de Preferencias (Editar -> Preferencias -> Javascript; deseleccionar "Habilitar Adobe Javascript").

Adobe provee un marco de trabajo para prohibir ciertas APIs de JAvascript. Si Javascript debe mantenerse habilitado, esta característica puede ser útil, si se conoce que ciertas APIs son vulnerables o utilizadas en ataques.

Prevenir que Internet Explorer abra automáticamente archivos PDF

El instalador de Adobe Reader y Acrobat configura a Internet Explorer para abrir archivos PDF automáticamente, sin interacción del lusuario. Este comportamiento puede ser revertido a una opción más segura, que alerte al usuario previamente, utilizando las siguientes líneas como archivo .REG:

Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOTAcroExch.Document.7]

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

Deshabilitar el despliegue de archivos PDF en el navegador web

La prevención de la apertura de archivos PDF dentro del navegador mitigará parcialmente esta vulnerabilidad. Si la solución es aplicada, también puede mitigar vulnerabilidades futuras.

Para prevenir que los archivos PDF sean abiertos de manera automática por un navegador web, haga lo siguiente:

1. Abrir Adobe Acrobat Reader

2. Abrir el menú Editar

3. Escoger el menú Preferencias

4. Escoger la sección de Internet

5. Deseleccionar la opción "Mostrar PDF en navegador"

No acceder a archivos PDF de fuentes no confiables

No abra archivos PDF inesperados o desconocidos, particularmente aquellos alojados en sitios web o

3. entregados como archivos adjuntos. Por favor, refiérase al tip de Ciber Seguridad ST04-010.
4. **Referencias**
5. **Referencias**

Actualización de seguridad disponible para Adobe Reader y Acrobat

Marco de trabajo para prohibición de ejecución de Javascript de Adobe Reader y Accrobat

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
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