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

Boletin de Seguridad UNAM-CERT-UNAM-CERT-2011-020 Actualizaciones de Adobe para Múltiples Vulnerabilidades

Adobe ha liberado el Boletín de Seguridad APSB11-30, que describe múltiples vulnerabilidades que afectan a Adobe Reader y Acrobat

- **Fecha de Liberación:** 16-Dic-2011
- **Ultima Revisión:** 16-Dic-2011
- **Fuente:** http://www.us-cert.gov/cas/techalerts/TA11-350A.html
- **Riesgo** Crítico
- **Problema de Vulnerabilidad** Local y remoto
- **Tipo de Vulnerabilidad** Ejecución remota de código y Elevación de privilegios

Sistemas Afectados

Multiple Multiple	Adobe Acrobat	<=	10.1.1
Multiple Multiple	Adobe Acrobat	<=	9.4.6

1. ## Descripción

   El Boletín de Seguridad de Adobe APSB11-30 y la Advertencia de Seguridad APSA11-04 describen una variedad de vulnerabilidades que afectan a Adobe Reader y Acrobat. Esta vulnerabilidades afectan a Reader y Acrobat 9.4.6 y versiones 9.x anteriores. Estas vulnerabilidades también afectan a Reader X y Acrobat X 10.1.1 y versiones anteriores 10.x.

   Un atacante podría explotar estas vulnerabilidades al convencer a un usuario de abrir un PDF especialmente diseñado. El plug-in para navegadores de Adobe Reader, que automáticamente abre documentos PDF alojados en sitios web, está disponible para múltiples navegadores y sistemas operativos.

   Adobe Reader X y Adobe Acrobat X serán actualizados en la siguiente actualización trimestral, agendada para el 10 de Enero de 2012.

   Detalles adicionales de la vulnerabilidad de corrupción de memoria U3D pueden ser encontrados en la Nota de Vulnerabilidad de US-CERT VU#75307.

2. ## Impacto

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

3. ## Solución

   Actualizar Reader

   Adobe ha liberado actualizaciones para corregir este problema. Se recomienda a los usuarios leer el boletín de seguridad de Adobe APSB11-30 y actualizar las versiones vulnerables de Adobe Reader y

Acrobat.

De manera adicional a la actualización, por favor considere las siguientes mitigaciones.

Deshabilitar Flash en Adobe Reader y Acrobat

Deshabilitar Flash en Adobe Reader mitigará los ataques que dependen de contenido Flash embebido en un archivo PDF. Deshabilitar soporte para 3D y Multimedia no corrige la vulnerabilidad directamente, pero sí provee mitigación adicional y resulta en mensajes de errores amigables para el usuario, en vez de una negación de servicio. Para deshabilitar Flash y soporte para 3D y Multimedia en Adobe Reader 9, borre, renombre, o elimine el acceso a los siguientes archivos:

Microsoft Windows

"%ProgramFiles%AdobeReader 9.0Readerauthplay.dll"
"%ProgramFiles%AdobeReader 9.0Reader t3d.dll"

Apple Mac OS X

"/Applications/Adobe Reader 9/Adobe Reader.app/Contents/Frameworks/AuthPlayLib.bundle"
"/Applications/Adobe Reader 9/Adobe Reader.app/Contents/Frameworks/Adobe3D.framework"

GNU/Linux (locations may vary among distributions)
"/opt/Adobe/Reader9/Reader/intellinux/lib/libauthplay.so"
"/opt/Adobe/Reader9/Reader/intellinux/lib/librt3d.so"

Las ubicaciones de los archivos pueden ser diferentes para Adobe Acrobat o para otros productos de Adobe que incluyan soporte para Flash, 3D y Multimedia. Deshabilitar estos plugins reducirá su funcionalidad y no protegerá contra contenido Flash que está alojado en sitios web. Dependiendo de la agenda de actualización para productos diferentes a Adobe Flash Player, considere dejar Flash y el soporte para 3D y Multimedia deshabilitados a menos que sean absolutamente necesarios.

Deshabilitar JavaScript en Adobe Reader y Acrobat

Deshabilitar JavaScript puede prevenir que algunos exploits resulten en ejecución de código remoto. Adobe JavaScript puede deshabilitarse utilizando el menú de Preferencias (Editar -> Preferencias -> JavaScript; deseleccionar Habilitar Acrobat JavaScript).

Adobe provee un framework para poner en lista negra ciertas APIs de JavaScript. Si JavaScript debe estar habilitado, este framework puede ser útil cuando APIs específicas son responsables de ciertos ataques, o vulnerables.

Prevenir que Internet Explorer abra automáticamente archivos PDF

El instalador para Adobe Reader y Acrobat configura a Internet Explorer para que automáticamente abra archivos PDF sin interacción alguna por parte del usuario. Este comportamiento puede ser revertido a la opción, más segura, que pide autorización del usuario, al importar lo siguiente como un archivo .REG:

------ Archivo comienza en la siguiente línea

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOTAcroExch.Document.7]
"EditFlags"=hex:00,00,00,00

------ Archivo termina en la línea anterior
```

Deshabilitar la ejecución de archivos PDF en el navegador web

Prevenir que los archivos PDF se abran dentro de un navegador web mitigará parcialmente esta vulnerabilidad. Si se aplica esta solución, puede mitigar vulnerabilidades futuras.

Para prevenir que los archivos PDF se ejecuten automáticamente en un navegador web, haga lo siguiente:

1. Abra Adobe Acrobat Reader

2. Abra el menú EDITAR

3. Escoja la opción PREFERENCIAS

4. Escoja la sección INTERNET

5. Deseleccione la caja con leyenda "Desplegar PDF en navegador".

Elimine o restrinja el acceso al archivo 3difr.x3d

Al eliminar o restringir el acceso al archivo 3difr.x3d, Adobe Reader y Acrobat no desplegarán contenido U3D, lo que ayuda a migitar esta vulnerabilidad. Los documentos PDF que utilizan el formato PRC para contenido 3D continuarán funcionando en plataformas Windows y Linux.

Para deshabilitar el soporte U3D en Adobe Reader 9 en Microsoft Windows, elimine o renombre el siguiente archivo:

"%ProgramFiles%AdobeReader 9.0Readerplug_ins3d difr.x3d"

Para Apple Mac OS X, elimine o renombre el siguiente archivo:

"/Applications/Adobe Reader 9/Adobe Reader.app/Contents/Frameworks/Adobe3D.framework"

Para GNU/Linux, elimine o nombre el siguiente archivo (la ubicación puede variar entre diferentes distribuciones):

"/opt/Adobe/Reader9/Reader/intellinux/plug_ins3d/3difr.x3d"

Las ubicaciones de los archivos pueden ser diferentes para Adobe Acrobat u otros productos o versiones de Adobe.

No abrir archivos PDF de fuentes no confiables

No abra archivos PDF inesperados o desconocidos, particularmente aquellos alojados en sitios web, o entregados como archivos adjuntos de correos electrónicos. Por favor, vea el Tip de Ciber Seguridad ST04-010.

4. Referencias

Actualización de seguridad disponible para Adobe Reader y Acrobat

Framework para añadir a listas negras JavaScript de Adobe Reader y Acrobat

Vulnerabilidad de corrupción de memoria U3D de Adobe Acrobat y Reader

Advertencia de Seguridad para Adobe Acrobat y Reader

La Subdirección de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Sergio A. Becerril (sbecerril 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