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

Boletin de Seguridad UNAM-CERT-2011-007 Actualización de Adobe para múltiples vulnerabilidades

Adobe ha publicado el boletín de seguridad APSB11-16, el cual describe múltiples vulnerabilidades que afectan a Adobe Reader y Acrobat. Adobe ha publicado el boletín de seguridad APSB11-17, el cual describe múltiples vulnerabilidades que afectan a Adobe Shockwave Player. Adoba ha publicado el boletín de seguridad APSB11-18, el cual describe múltiples vulnerabilidades que afectan a Adobe Flash Player.

- **Fecha de Liberación:** 15-Jun-2011
- **Ultima Revisión:** 15-Jun-2011
- **Fuente:** US-CERT
- **CVE ID:** TA11-166A
- **Riesgo** Moderado
- **Problema de Vulnerabilidad** Remoto
- **Tipo de Vulnerabilidad** Ejecución Remota de Código

Sistemas Afectados

Microsoft Windows	Adobe Reader	< 10.x
Multiple Multiple	Adobe Acrobat	< 8.2.6
Multiple Multiple	Adobe Acrobat	< 9.4.3
Multiple Multiple	Adobe Flash Player	< 10.3.181.23
Multiple Multiple	Adobe Flash Player	< 10.3.185.23
Multiple Multiple	Adobe Macromedia Shockwave Player	< 11.5.9.620
Multiple Multiple	Adobe Reader	< 10.x
Multiple Multiple	Adobe Reader	< 8.2.6
Multiple Multiple	Adobe Reader	< 9.4.3

1. Descripción

El boletín de seguridad de Adobe APSB11-16 describe un número de vulnerabilidades que afectan a Adobe Reader y Acrobat. Estas vulnerabilidades afectan Reader y Acrobat 9.3.4, versiones anteriores a 9.x, 8.2.6 y versiones anteriores a 8.x. Estas vulnerabilidades también afectan Reader X y Acrobat X 10.0.3, 10.0.1 y versiones anteriores a 10.x.

Un atacante podría aprovechar esta vulnerabilidad, convenciendo a un usuario en abrir un archivo PDF especialmente diseñado. El plug-in del explorador de Adobe Reader, automáticamente puede abrir documentos PDF alojados en un sitio Web. Esta disponible en múltiples navegadores y sistemas operativos.

El boletín de seguridad de Adobe APSB11-17 describe un número de vulnerabilidades que afectan a Adobe Shockwave Player. Estas vulnerabilidades afectan a Shockwave Player 11.5.9.620 y versiones anteriores.

Un atacante podría aprovechar esta vulnerabilidad, convenciendo a un usuario en abrir contenido Shockwave especialmente diseñado. El contenido Shockwave esta comúnmente alojado en páginas Web, pero también puede embeberse en PDF y otros documentos o como un archivo independiente.

El boletín de seguridad de Adobe APSB11-18 describe un número de vulnerabilidades que afectan a Adobe Flash Player. Estas vulnerabilidades afectan a Flash Player 10.3.181.23 y versiones anteriores para sistemas operativos de Windows, Macintosh, Linux y Solaris. Estas vulnerabilidades también afectan a Flash Player 10.3.185 y versiones anteriores de Android.

Un atacante podría aprovechar esta vulnerabilidad, convenciendo a un usuario en abrir un archivo de Flash especialmente diseñado. El contenido Flash esta comúnmente alojado en páginas Web, pero también puede embeberse en PDF y otros documentos o como un archivo independiente.

2. Impacto

Estas vulnerabilidades podrían permitir a un atacante remoto ejecutar código arbitrario, escribir archivos o directorios arbitrarios al archivo del sistema, escalar privilegios locales, o causar una denegación de servicio en un sistema afectado, como resultado de que un usuario haya abierto un archivo PDF malicioso.

Si un usuario abre un archivo especialmente diseñado con contenido Shockwave, un atacante remoto puede ejecutar código arbitrario.

Si un usuario abre un archivo especialmente diseñado con contenido Flash, un atacante remoto puede ejecutar código arbitrario.

3. Solución

Actualizar Adobe

Adoba ha liberado actualizaciones para solucionar este problema. Los usuarios están invitados a leer el boletín de seguridad de Adobe APSB11-16 y actualizar las versiones vulnerables de Adobe Reader y Acrobat.

Actualizar Adobe Shockwave Player

Adoba ha liberado actualizaciones para solucionar este problema. Los usuarios están invitados a leer el boletín de seguridad de Adobe APSB11-17 y actualizar las versiones vulnerables de Adobe Shockwave Player.

Actualizar Adobe Flash Player

Adobe ha liberado actualizaciones para solucionar este problema. Los usuarios están invitados a leer el boletín de seguridad de Adobe APSB11-18 y actualizar las versiones vulnerables de Adobe Flash Player.

Desactivar Flash en tu navegador Web

Desinstalar Flash o restringir que sitios están permitidos para correr Flash.
En la medida de lo posible, solo ejecutar contenido Flash confiable en dominios confiables.
Para más información, consulte Securing Your Web Browser .

Desactivar Flash en Adobe Reader y Acrobat

Desactivando Flash en Adobe Reader mitigará los ataques que se basan en contenido Flash embebido en un archivo PDF. Desactivando soporte para 3D y Multimedia no aborda directamente la vulnerabilidad, pero provee una mitigación adicional y resulta en un error más fácil de manejar en vez de un accidente. Para deshabilitar Flash y soporte para 3D y Multimedia en Adobe Reader 9, borrar, renombrar o remover acceso a estos archivos:

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

Apple Mac OS X
"/Applications/Adobe Reader 9/AdobeReader.app/Contents/Frameworks/AuthPlayLib.bundle"
"/Applications/Adobe Reader 9/AdobeReader.app/Contents/Frameworks/Adobe3D.framework"

GNU/Linux (localidades pueden variar de acuerdo a distribuciones)
"/opt/Adobe/Reader9/Reader/intellinux/lib/libauthplay.so"
"/opt/Adobe/Reader9/Reader/intellinux/lib/librt3d.so"

Las ubicaciones de archivos pueden ser diferente para Adobe y otros productos Adobe que incluyen Flash y soporte para 3D y Multimedia. Desactivando estos plugins reducirá la funcionalidad y no protegerá contra contenido Flash alojado en sitios Web. Dependiendo del calendario de actualización para productos distintos de Flash Player, considerar dejar desactivado Flash y el soporte 3D y Multimedia a menos que sea absolutamente necesario.

Desactivar JavaScript en Adobe Reader y Acrobat

Desactivar JavaScript puede prevenir algunos ataques resultantes de ejecución de código remoto. Acrobat Javascript puede ser desactivado usando el menú de Preferencias. (Edit -> Preferences -> JavaScript; deseleccionar Enable Acrobat JavaScript).

Adobe provee un framework a las lista negra especifica de JavaScript APIs. Si JavaScript debe estar habilitados, esta característica puede ser útil cuando APIs especificas son conocidas por ser vulnerables o usadas en ataques.

Evitar que Internet Explorer abra automáticamente archivos PDF.

El instalador de Adobe Reader y Acrobat configura Internet Explorer para que automáticamente abra archivos PDF sin ninguna interacción del usuario. Este comportamiento se puede revertir a una opción segura que pide al usuario la importación de lo siguiente como un archivo .REG:

Versión de Windows Registry Editor 5.00

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

Desactivar la visualización de archivos en el navegador Web

Prevenir que archivos PDF se abran dentro del navegador Web parcialmente mitigara esta vulnerabilidad. Si esta solución se aplica, también puede mitigar futuras vulnerabilidades.

Para prevenir que archivos PDF se abran dentro de un navegador Web, realizar lo siguiente:

1. Abrir Adobe Acrobat Reader
2. Abrir el menú Editar
3. Elegir la opción Preferencias
4. Elegir la sección Internet
5. Desactivar la casilla de texto Mostrar PDF en navegador

No acceder a archivos PDF desde fuentes no confiables

No abrir archivos PDF no familiares o inesperados, particularmente aquellos alojados en sitios Web o entregados como un adjunto de correos electrónicos. Por favor consultar Cyber Security Tip ST04-010 .

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

- Francisco Carlos Martínez Godínez (fmartinez at seguridad dot unam dot mx)
- José Roberto Sánchez Soledad (rsanchez at seguridad dot unam dot mx)
- Javier Santillán Arenas (jsantillan 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