Boletin de Seguridad UNAM-CERT-2012-007 Actualizaciones de seguridad y mejoras en la arquitectura de Adobe Reader y Acrobat

Adobe ha publicado el Boletín de Seguridad APSB12-08 que describe multiples vulnerabilidades que afectan a Acrobat Reader y a Acrobat. Como parte de esta actualización, Adobe Reader y Acrobat 9.x utilizarán el plug-in Flash Player para navegador web, en lugar del componente Authplay. Además, Reader y Acrobat ahora deshabilitan de manera predeterminada el renderizado de contenido 3D.

- **Fecha de Liberación:** 11-Abr-2012
- **Ultima Revisión:** 11-Abr-2012
- **Fuente:**
- **Problema de Vulnerabilidad** Local y remoto
- **Tipo de Vulnerabilidad** Múltiples vulnerabilidades

Sistemas Afectados

Multiple Multiple	Adobe Acrobat	<=	10.1.2
Multiple Multiple	Adobe Acrobat	<=	9.5
Multiple Multiple	Adobe Reader	<=	10.1.2
Multiple Multiple	Adobe Reader	<=	9.5

1. Descripción

El Boletín de Seguridad APSB12-08 describe una serie de vulnerabilidades que afectan a Adobe Reader y a Acrobat. Estas vulnerabilidades afectan versiones 9.x (hasta la 9.5) de Adobe Reader y de Acrobat, y versiones anteriores a la 10.1.3 de Reader X y Acrobat X.

El blog ASSET, de Adobe, provee detalles adicionales sobre los nuevos cambios en la arquitectura de seguridad para Adobe Reader y Acrobat. Adobe Reader y Acrobat 9.5.1 utilizarán la versión del plug-in Adobe Flash Player instalada en el sistema de los usuarios, en lugar del componente Authplay que se incluye con Adobe Reader y Acrobat. Este cambio ayuda a limitar el número de ambientes de ejecución Flash, vulnerables y desactualizados, disponibles para un atacante. Adobe Reader y Acrobat 9.5.1 también deshabilitan de manera predeterminada el renderizado de contenido 3D debido a que los componentes de renderizado 3D han presentado vulnerabilidades constantemente.

US-CERT recomienda que los usuarios de Flash actualicen a la última versión de Adobe Flash Player y activen las actualizaciones automáticas.

Un atacante podría aprovechar estas vulnerabilidades al convencer a un usuario de abrir un archivo PDF especialmente diseñado. Esto puede suceder automáticamente como resultado de ver una página web.

2. Impacto

Estas vulnerabilidades podrían permitir a un atacante ejecutar código arbitrario de manera remota, crear archivos o carpetas arbitrarios en el sistema de archivos, escalar privilegios locales o causar una denegación de servicio en un sistema afectado como resultado de que un usuario abra un archivo PDF malicioso.

3. Solución

Actualizar Reader

Adobe ha publicado las actualizaciones correspondientes. Se recomienda a los usuarios leer el Boletín de Seguridad APSB12-08 de Adobe, y actualizar las versiones vulnerables de Adobe Reader y Acrobat.

Además de la actualización, por favor considere las siguientes mitigaciones:

Deshabilitar JavaScript en Adobe Reader y Acrobat

Deshabilitar JavaScript puede prevenir que algunos exploits logren ejecución de código. Puede deshabilitar Acrobat JavaScript usando el menú Preferencias (Edición -> Preferencias -> JavaScript; desactivar "Habilitar Acrobat Javascript").

Adobe provee una plataforma (JavaScript Blacklist Framework) para poner en la lista negra APIs de Javascript específicas. Si JavaScript debe estar habilitado, ésta plataforma puede ser útil cuando se sabe que APIs específicas son vulnerables o usadas en ataques.

Prevenir que Internet Explorer abra automáticamente archivos PDF

El instalador de Adobe Reader y Acrobat configura Internet Explorer para abrir automáticamente archivos PDF sin intervención del usuario. Este comportamiento puede ser cambiado a uno más seguro, en el que se le solicita autorización al usuario, importando como archivo .REG lo siguiente:

```
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

Prevenir que archivos PDF sean abiertos dentro del navegador mitigará parcialmente esta vulnerabilidad. Aplicar esta solución puede a su vez mitigar futuras vulnerabilidades.

Para prevenir la apertura automática de archivos PDF en un navegador web, haga lo siguiente:

1. Abra Adobe Acrobat Reader.
2. Abra el menú Edición.
3. Eliga la opción Preferencias.
4. Eliga la opción Internet
5. Desactive la casilla "Abrir PDF en el navegador".

No acceda a archivos PDF que provengan de fuentes no confiables.

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

4. Referencias

* Actualización de seguridad disponible para Adobe Reader y Acrobat

* Adobe Reader y Acrobat JavaScript Blacklist Framework

* Antecedentes del Security Bulletin APSB12-08

* Adobe Flash Player

* Vulnerabilidad en Adobe Flash afecta Flash Player y otros productos de Adobe

* Notas de la vulnerabilidad con consejos para deshabilitar el renderizado 3D

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

- Jesús Sánchez (jsanchez 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