UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA-UNAM

Boletin de Seguridad UNAM-CERT-2010-013

Vulnerabilidad en Adobe Flash, Reader, y Acrobat

De acuerdo con Adobe, existe una vulnerabilidad en Adobe Flash. Ésta vulnerabilidad afecta a Flash Player, Reader, Acrobat, y posiblemente otros productos que soportan Flash. Un atacante a distancia podría aprovechar esta vulnerabildad para ejecutar código arbitrario.

Fecha de Liberación: 8-Jun-2010

Ultima Revisión: 15-Jun-2010

Fuente: US-CERT

CVE ID: **TA10-159A**

Riesgo

Moderado

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Ejecución Remota de Código

I. Sistemas afectados

* Adobe Flash Player 10.0.45.2 y versiones 10.x anteriores

* Adobe Flash Player 9.0.262 y versiones 9.x anteriores

* Adobe Reader 9.3.2 y versiones 9.x anteriores

* Adobe Acrobat 9.3.2 y versiones 9.x anteriores

Otros productos de Adobe que soportan Flash pueden también ser vulnerables.

II. Descripción

Adobe Security Advisory APSA10-01 describe una vulnerabildad en Adobe Flash que afecta Flash Player, Reader y Acrobat. Puede afectar también a otros productos que soporten Flash independientemente, tales como Photoshop, Photoshop Lightroom, Freehand MX y Fireworks.

Un atacante podría aprovechar esta vulnerabilidad convenciendo a un usuario de abrir contenido Flash especialmente diseñado. El contenido Flash se aloja comunmente en una página web pero puede también estar incrustado en documentos PDF u otros, o proporcionado en un archivo independiente.

Como se señala en APSA10-01, "Hay reportes de que esta vulnerabilidad está siendo activamente aprovechada en la realidad en contra de Adobe Flash Player, Adobe Reader y Acrobat."

Información adicional se encuentra disponible en US-CERT Vulnerability Note VU#486225.

III. Impacto

Si un usuario abre contenido Flash especialmente diseñado, un atacante a distancia puede ser capaz de ejecutar código arbitrario.

IV. Solución

Actualización

Adobe Security Advisory APSA10-01 sugiere actualizar a la versión candidata de Flash Player 10.1.

Deshabilitar Flash en su navegador web

Desistalar Flash o restringir los sitios que tienen permitido ejecutar Flash. En la medida de lo posible, sólo ejecutar contenido Flash de confianza o en sitios de confianza. Para más información consultar la referencia "Securing Your Web Browser".

Deshabilitar Flash en Adobe Reader y Acrobat

Deshabilitar Flash en Adobe Reader mitigará los ataques que se basan en contenido flash incrustado en un archivo PDF. Deshabilitar soporte 3D y Multimedia no aborda directamente esta vulnerabilidad pero provee mitigación adicional y se refleja en un mensaje de error más amigable.

Para deshabilitar el soporte Flash y 3D & 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 (Las ubicaciones pueden variar entre distribuciones)

"/opt/Adobe/Reader9/Reader/intellinux/lib/libauthplay.so"

"/opt/Adobe/Reader9/Reader/intellinux/lib/librt3d.so"

La ubicación de los archivos puede ser diferente para Adobe Acrobat u otros productos de Adobe que incluyen soporte Flash y 3D & Multimedia.

Desabilitar estos plugins reducirá la funcionalidad y no protejerá contra contenido Flash alojado en sitios web. Dependiendo del calendario de actualización de los productos que no sean Flash Player, considere mantener el soporte Flash y 3D & Multimedia deshabilitado a menos que sea absolutamente requerido.

Evitar que Internet Explorer abra automáticamente documentos PDF

El instalador para Adobe Reader y Acrobat configura Internet Explorer para que abra automaticamente archivos PDF sin ninguna interacción por parte del usuario. Éste comportamiento puede ser revertido, a una opción más segura que consulte al usuario, importando lo siguiente como un archivo .REG:

Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOTAcroExch.Document.7]

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

Deshabilitar la visualización de documentos PDF en el navegador web

Prevenir que los documentos PDF sean abiertos dentro del navegador web mitigará parcialmente esta vulnerabilidad. Si ésta solución es aplicada, puede incluso mitigar futuras vulnerabilidades.

Para evitar que los documentos PDF sean abiertos automáticamente en el navegador web, haga lo siguiente:

1. Abrir Adobe Acrobat Reader.

2. Abrir el menú Edición.

3. Elegir la opción Preferencias.

4. Elegir la sección Internet.

5. Desactivar la casilla de verificación "Mostrar PDF en explorador".

Deshabilitar JavaScript en Adobe Reader y Acrobat

Deshabilitar JavaScript provee protección adicional contra algunos ataques.

Acrobat JavaScript puede ser deshabilitado usando el menú Preferencias (Edición -> Preferencias -> JavaScript; Deshabilitar "Activar JavaScript para Acrobat").

Habilitar DEP en Microsoft Windows

Considere habilitar Data Execution Prevention (DEP) en versiones soportadas de Windows.

DEP no debe tomarse como una solución completa, pero puede mitigar la ejecución de código suministrado por el atacante en algunos casos. Microsoft ha pubilcado información técnica detallada acerca de DEP en las entradas "Understanding DEP as a mitigation technology", parte 1 y 2, del blog "Security Research & Defense". El uso de DEP se debe considerar en conjunción con la aplicación de parches u otras mitigaciones descritas en este documento.

No acceder a documentos PDF de fuentes no confiables

No abrir documentos PDF desconocidos o inesperados, particularmente aquellos alojados en sitios web o que se entreguen como archivos adjuntos de correo electrónico.

Consulte "Cyber Security Tip ST04-010".

V. Referencias

* Security Advisory for Flash Player, Adobe Reader and Acrobat

* Adobe Labs - Flash Player 10 pre-release

* US-CERT Vulnerability Note VU#486225 -

* Securing Your Web Browser

* Understanding DEP as a mitigation technology part 1

* Understanding DEP as a mitigation technology part 2

La versión más reciente de este documento puede ser encontrada en:

El Departamento de Seguridad en Cómputo/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
Departamento de Seguridad en Cómputo
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