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

Boletin de Seguridad UNAM-CERT-2010-026 Vulnerabilidad no especificada permite ejecución de código en Adobe Flash

Adobe Flash contiene una vulnerabilidad no especificada que puede permitir a un atacante remoto sin autenticar la ejecución de código arbitrario.

- **Fecha de Liberación:** 14-Sep-2010
- **Ultima Revisión:** 20-Sep-2010
- **Fuente:** CERT/CC
- **Riesgo** Alto
- **Problema de Vulnerabilidad** Remoto
- **Tipo de Vulnerabilidad** Ejecución Remota de Código

Sistemas Afectados

Multiple	Multiple	Windows	<=	10.1.82.76

1. Descripción

Adobe Flash contiene una vulnerabilidad que puede originar un error en la memoria y permitir ejecución arbitraria de código.

2. Impacto

Convenciendo a un usuario a visualizar un archivo HTML (por ejemplo, una página Web, un mensaje por correo electrónico en HTML o un archivo adjunto HTML), un documento en PDF, un documento de Microsoft Office o cualquier otro documento que soporte contenidos SWF, un atacante podría ser capaz de ejecutar código arbitrario. La vulnerabilidad anunciada afecta a Flash Player 10.1.82.76 y versiones anteriores para Windows, Macintosh, Linux, Solaris, Flash Player 10.1.92.10 para Android así como Adobe Reader y Acrobad 9.3.4 así como versiones anteriores.

3. Solución

Hasta este momento no se tiene una solución para este problema. Por favor considere las siguientes recomendaciones.

Deshabilitar Flash en el navegador Web

Deshabilitar Flash o activar de forma selectiva el contenido de Flash como se describe en asegurando tu navegador Web (http://www.us-cert.gov/reading_room/securing_browser/).

Deshabilitar Flash y 3D & Multimedia que es soportado en Adobe Reader 9

Flash y 3d & Multimedia son implementadas como bibliotecas de plug ins y soportadas en Adobe Reader. Deshabilitando Flash en Adobe Reader solo mitigará a los atacantes que usen archivos SWF alojados en documentos PDF. Deshabilitando el soporte de 3D & Multimedia no evitará directamente la vulnerabilidad pero proporcionará una mitigación adicional y como resultado la no explotación de

la vulnerabilidad así como un mensaje de error más amistoso.

Para desactivar el soporte de Flash y 3D & Multimedia en Adobe Reader 9 para Microsoft Windows, es necesario borrar o renombrar estos archivos:

"%ProgramFiles%AdobeReader 9.0Readerauthplay.dll"

"%ProgramFiles%AdobeReader 9.0Reader

t3d.dll"

Para GNU/Linux, borrar o renombrar estos archivos (los ubicación pueden variar dependiendo de la distribución)

"/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 para Flash y 3D & Multimedia. Deshabilitando estos plug ins reducirá la funcionalidad y no protegerá contra archivos SWF alojados en sitios Web. Dependiendo del calendario de actualizaciones para los productos de Adobe como Flash Player, es necesario mantener el soporte deshabilitado para Flash y 3D & Multimedia a menos de que sea absolutamente requerido.

Eliminar Flash

Adobe ha proporcionado una TechNote (http://kb2.adobe.com/cps/141/tn_14157.html) con utilerías para desinstalar el plug in de Flash Player y controles ActiveX para Windows y Mac OS. Eliminando estos componentes es posible mitigar los vectores de ataque en navegadores Web para esta vulnerabilidad. Esto no eliminará las instancias de Flash Player que se encuentran instaladas con Adobe Reader 9 u otros productos de Adobe.

Deshabilitar JavaScript en Adobe Reader y Acrobat

Deshabilitando JavaScript puede ayudar a mitigar algunas técnicas usadas en los vectores de ataque para Adobe Reader.

Para deshabilitar JavaScript en Adobe Reader:

1. Abrir Adobe Acrobat Reader.

2. Abrir el menú de Editar.

3. Elegir la opción Preferencias

4. Elegir la sección de JavaScript.

5. Desmarcar la opción Habilitar Acrobat JavaScript.

Deshabilitando JavaScript no resolverá las vulnerabilidades, solamente deshabilitará la vulnerabilidad para el componente de JavaScript. Cuando JavaScript es deshabilitado en Adobe Reader y Acrobat, se

muestra un mensaje de habilitar JavaScript cuando se abre un documento PDF que contenga JavaScript.

Evitar que Internet Explorer abra documentos PDF automáticamente

El instalador de Adobe Reader y Acrobat configura Internet Explorar para que abra archivos PDF automáticamente sin la interacción del usuario. Este comportamiento puede ser revertido con el siguiente archivo que debe ser importado como un archivo .REG:

Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOTAcroExch.Document.7]

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

Deshabilitar que los documentos PDF sean mostrados en el navegador Web

Evitando que los documentos PDF sean abiertos dentro de un navegador web reduce el ataque. Si esta solución es aplicada a las versiones actualizadas de Adobe Reader y Acrobat, puede proteger contra futuras vulnerabilidades.

Para evitar que los documentos PDF sean abiertos automáticamente desde el navegador Web con Adobe Reader.

1. Abrir Adobe Acrobat Reader.

2. Abrir el menú Edit.

3. Elegir la opción de Preferencias.

4. Elegir la sección Internet.

5. Desmarcar la opción de Mostrar PDF en el navegador.

Habilitar DEP (Data Execution Prevention) en Microsoft Windows

Considerar el habilitar Data Execution Prevention (DEP) soportado en versiones de Windows. DEP no debe ser considerada como una solución completa, pero puede mitigar la ejecución de ataques de código en algunos casos. Microsoft ha publicado información técnica detallada sobre DEP en su publicación del blog Security Research & Defense Entendiendo DEP como una tecnología de mitigación Parte1 y Parte2 . DEP debe ser usado en conjunto con la aplicación de parches u otras formas de mitigar descritas en este documento.

4. ## Referencias

http://www.adobe.com/support/security/advisories/apsa10-03.html

http://blogs.adobe.com/psirt/2010/09/security-advisory-for-adobe-flash-player-apsa10-03.html

El Departamento de Seguridad en Cómputo/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Pablo Antonio Lorenzana Gutiérrez (plorenzana 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