UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2008−004

Vulnerabilidades en Adobe Reader y Acrobat

Adobe ha publicado un aviso de seguridad APSA08−01 que describe múltiples vulnerabilidades que afectan Adobe Reader y Acrobat. Lo más grave de estas vulnerabilidades es que un atacante podría ejecutar código de su elección de forma remota.

Fecha de Liberación: 12 de Febrero de 2008

Ultima Revisión: 12 de Febrero de 2008

Fuente: CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, asi como foros y listas de discusion.

Riesgo

Crítico

Problema de Vulnerabilidad

Local y remoto

Tipo de Vulnerabilidad

Ejecución Remota de Código

I. Sistemas Afectados

- Adobe Reader versión 8.1.1 y anteriores.
- Adobe Acrobat Professional, 3D, 8.1.1 en su versión estándar

II. Descripción

El aviso de Seguridad de Adobe APSA08−01 describe una serie de vulnerabilidades que afectan a la familia de productos de Adobe Acrobat, incluyendo Adobe Reader. Las versiones 8.1.1 y anteriores son afectadas. Para más detalles puede consultar la Base de Datos de Notas de Vulnerabilidad del US−CERT.

Un intruso podría explotar esta vulnerabilidad al convencer a un usuario de ejecutar un archivo en formato PDF (Portable Document Format) especialmente modificado. Otra modalidad puede ser convenciendo al usuario para que visite un sitio Web con un navegador que tenga integrado Acrobat; el ataque podría ser exitoso con tan sólo acceder al sitio Web.

Por lo menos una de estas vulnerabilidades sigue siendo explotada. El Handler's Diary del SANS Internet Storm Center contiene más información al respecto.

III. Impacto

El impacto de esta vulnerabilidad es variable. Lo más grave de esta vulnerabilidad es que un intruso podría ejecutar código arbitrario de forma remota.

IV. Solución

- Actualizar la verside Acrobat

  Actualizar Adobe Reader o Acrobat a la versión 8.1.2 de acuerdo a la información en el Aviso de Seguridad de Adobe APSA08−01.

- Deshabilitar en el navegador Web el despliegue documentos PDF

  El prevenir que documentos PDF se abran dentro de un navegador Web podría mitigar esta vulnerabilidad. Aplicando la siguiente solución temporal en conjunto con la actualización del software podría prevenir que vulnerabilidades similares sean explotadas automáticamente.

  Para prevenir que documentos PDF sean abiertos automáticamente en un navegador Web con Acrobat o Reader:

  1. Abra Adobe Acrobat o Adobe Reader.
  2. Abra el menú Edición.
  3. Elija la opción Preferencias.
  4. Elija la sección Internet.
  5. De−seleccione el cuadro de verificación "Mostrar PDF en explorador".

- Deshabilitar la visualización automática de documentos PDF en Microsoft Internet Explorer

  Para deshabilitar la apertura automática de archivos PDF en Microsoft Internet Explorer (IE), se requiere de un segundo paso. Para configurar que IE pida autorización para abrir un archivo PDF, deshabilite la característica "Mostrar PDF en explorador" (como se describe anteriormente) y después realice los siguientes cambios en el registro de Windows:

  Windows Registry Editor Version 5.00

  [HKEY_CLASSES_ROOT\AcroExch.Document.7]

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

- Deshabilite JavaScript en Adobe Reader y Acrobat

  Deshabilitar JavaScript en Adobe Reader y Acrobat podría prevenir que esta vulnerabilidad sea explotada. En Acrobat Reader, JavaScript puede ser deshabilitada en el cuadro de preferencias General (Edición −−> Preferencias −−> JavaScript, de−seleccione Habilitar Acrobat JavaScript).

V. Referencias

- Notas de Vulnerabilidad del US−CERT para el aviso de Seguridad de APSA08−01 − http://www.kb.cert.org/vuls/byid?searchview&query=APSA08−01
- Asegurando tu navegador Web − http://www.us−cert.gov/reading_room/securing_browser/
- Aviso de Seguridad de Adobe APSA08−01 − http://www.adobe.com/support/security/advisories/apsa08−01.html
- Notas de Liberación de Adobe Reader 8.1.2 − http://www.adobe.com/go/kb403079
- SANS Internet Storm Center Handler's Diary − http://isc.sans.org/diary.html?storyid=3958
- Configurando el Explorador de Windows − Registry EditFlags − http://mc−computing.com/WinExplorer/WinExplorerEditFlags.htm
- Internet Explorer Abre Archivos .exe en lugar de Descargarlos − http://support.microsoft.com/kb/140991
- Abriendo Documentos de Office en IE − http://blogs.msdn.com/omars/archive/2004/04/29/123181.aspx

---

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

- Jesús Ramón Jiménez Rojas (jrojas at seguridad dot unam dot mx)
- Israel Becerril Sierra (ibecerril 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 43