UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−011

Vulnerabilidades en Productos Adobe Macromedia Flash

Existen vulnerabilidades críticas en el reproductor de Macromedia Flash y en software relacionado. La explotación de estas vulnerabilidades podría permitir a un intruso remoto no autenticado ejecutar código arbitrario o causar una negación de servicio en un sistema vulnerable.

Fecha de Liberación:	16 de Marzo de 2006
Ultima Revisión:	16 de Marzo de 2006
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión

Sistemas Afectados

Linux	**Adobe Macromedia Shockwave Player**	==10.1.0.11 y anteriores
Linux	**Breeze Meeting Add−In**	==5.1 y anteriores
Linux	**Flash**	==Basic
Linux	**Flash Debug Player**	==7.0.14.0 y anteriores
Linux	**Flash MX**	==2004
Linux	**Flash Player**	==8.0.22.0 y anteriores
Linux	**Flash Professional**	==8
Linux	**Flex**	==1.5
Mac OS X	**Adobe Macromedia Shockwave Player**	==10.1.0.11 y anteriores
Mac OS X	**Breeze Meeting Add−In**	==5.1 y anteriores
Mac OS X	**Flash**	==Basic
Mac OS X	**Flash Debug Player**	==

		7.0.14.0 y anteriores
Mac OS X	**Flash MX**	==2004
Mac OS X	**Flash Player**	==8.0.22.0 y anteriores
Mac OS X	**Flash Professional**	==8
Mac OS X	**Flex**	==1.5
Microsoft Windows	**Adobe Macromedia Shockwave Player**	==10.1.0.11 y anteriores
Microsoft Windows	**Breeze Meeting Add−In**	==5.1 y anteriores
Microsoft Windows	**Flash**	==Basic
Microsoft Windows	**Flash Debug Player**	==7.0.14.0 y anteriores
Microsoft Windows	**Flash MX**	==2004
Microsoft Windows	**Flash Player**	==8.0.22.0 y anteriores
Microsoft Windows	**Flash Professional**	==8
Microsoft Windows	**Flex**	==1.5
Solaris	**Adobe Macromedia Shockwave Player**	==10.1.0.11 y anteriores
Solaris	**Breeze Meeting Add−In**	==5.1 y anteriores
Solaris	**Flash**	==Basic
Solaris	**Flash Debug Player**	==7.0.14.0 y anteriores
Solaris	**Flash MX**	==2004
Solaris	**Flash Player**	==8.0.22.0 y anteriores
Solaris	**Flash Professional**	==8
Solaris	**Flex**	==1.5

Riesgo

Crítico

Problema de Vulnerabilidad

Local y remoto

Tipo de Vulnerabilidad

Ejecución remota de código y negación de servicio

I. **Descripción**

El Boletín de Seguridad de Adobe APSB06−03 cubre vulnerabilidades en reproductores de Macromedia Flash y software relacionado. Mayor información está disponible en la siguiente Nota de Vulnerabilidad del US−CERT:

- **VU#945060 − Productos Adobe Macromedia Flash contienen múltiples vulnerabilidades**

  Varias vulnerabilidades en productos Adobe Macromedia Flash podrían permitir a un intruso remoto ejecutar código arbitrario en un sistema vulnerable.
  (CVE−2006−0024)

  Varios sistemas operativos incluyendo Microsoft Windows (consulte el Aviso de Seguridad de Microsoft 916208), tienen versiones vulnerables de Flash instaladas de forma predeterminada. Los sistemas con navegadores de Web habilitados con Flash son vulnerables. Un intruso podría almacenar un archivo de Flash creado de forma maliciosa en un sitio Web y convencer a un usuario de visitar el sitio.

II. Impacto

Un intruso remoto no autenticado podría ejecutar código arbitrario con los privilegios del usuario. Si el usuario ha iniciado sesión con privilegios administrativos, el intruso podría tomar el control completo de un sistema afectado. Un intruso podría ser capaz de causar una negación de servicio.

III. Solución

- **Aplicar una actualización**

  Adobe ha proporcionado las actualizaciones para estas vulnerabilidades en APBS06−03

- **Deshabilitar Flash**

  Consulte el Aviso de Seguridad de Microsoft 916208 para obtener instrucciones de como deshabilitar Flash en Microsoft Windows. Para otros sistemas operativos y navegadores Web contacte a su distribuidor apropiado.

IV. Apéndice A. Referencias

- Macromedia − APSB06−03: Flash Player Update to Address Security Vulnerabilities − <http://www.macromedia.com/devnet/security/security_zone/apsb06−03.html>
- Nota de Vulnerabilidad del US−CERT VU#945060 − <http://www.kb.cert.org/vuls/id/945060>
- CVE−2006−0024 − <http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0024>
- Aviso de Seguridad de Microsoft − <http://www.microsoft.com/technet/security/advisory/916208.mspx>

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)

UNAM−CERT
Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Cómputo
E−Mail: seguridad@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