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

# Boletin de Seguridad UNAM-CERT-2010-019 Vulnerabilidades en Adobe Flash y Air

De acuerdo con el Boletín de seguridad de Adobe APSB10-16, hay vulnerabilidades en Adobe Flash y AIR. Estas vulnerabilidades afectan a Flash Player, AIR, y posiblemente otros productos soportados por Flash. Un atacante remoto podría explotar estas vulnerabilidades para ejecutar código arbitrario.

- **Fecha de Liberación:** 11-Ago-2010
- **Ultima Revisión:** 13-Ago-2010
- **Fuente:** US-CERT
- **Riesgo** Importante
- **Problema de Vulnerabilidad** Remoto
- **Tipo de Vulnerabilidad** Ejecución Remota de Código

## Sistemas Afectados

| | | | |
|---|---|---|---|
| Multiple Multiple | Adobe AIR | <= | 2.0.2.12610 |
| Multiple Multiple | Adobe Reader | <= | 9.3.3 |
| Multiple Multiple | Adobe Reader | <= | 9.x |
| Multiple Multiple | Flash Player | <= | 10.1.53.64 |
| Multiple Multiple | Flash Player | <= | 9.0.277.0 |

## 1. Solución

Actualización de Flash y AIR

El boletín de seguridad de Adobe APSB10-16 recomienda actualizar a Flash Player 10.1.82.76 o 9.0.280 y AIR 2.0.3. Esto actualizará el plug-in del navegador y el control ActiveX de Flash, así como el de AIR. Sin embargo, esto no actualiza el soporte Flash en Adobe Reader, Acrobat, u otros productos.

Para reducir la exposición a estas y otras vulnerabilidades de Flash, considerar las siguientes técnicas de mitigación.

- Desactivar Flash en su navegador

- Desinstalar Flash o restringir los sitios que están autorizados a ejecutar Flash. En la medida de lo posible, solamente ejecutar contenido Flash en dominios de confianza. Para obtener más información, vea "Asegurando su navegador web".

Soluciones adicionales están disponibles en la nota de la vulnerabilidad 660993 del US-CERT.

## 2. Descripción

El boletín de seguridad de Adobe APSB10-16 describe las vulnerabilidades de Adobe Flash que afectan a Flash Player y AIR. Estas vulnerabilidades también pueden afectar a otros productos que independientemente soportan Flash, como Adobe Reader, Acrobat, Photoshop, Photoshop Lightroom, MX Freehand y Fireworks.

Un atacante podría explotar estas vulnerabilidades convenciendo a un usuario para que abra contenido de Flash especialmente diseñado. Este contenido es comúnmente alojado en una página web, pero también se pueden incrustar en un PDF y otros documentos o proveerse como un archivo independiente.

## 3. Impacto

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

Referencias

* Boletín de seguridad de Adobe APSB10-16 -

http://www.adobe.com/support/security/bulletins/apsb10-16.html

* Vulnerabilidad del US-CERT VU # 660993 -

http://www.kb.cert.org/vuls/id/660993

* Asegurando su navegador web -

http://www.us-cert.gov/reading_room/securing_browser

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

- Javier Santillán Arenas (jsantillan 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
Subsecretaria 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