

Boletín de Seguridad UNAM-CERT-2015-011

Actualizaciones de seguridad disponibles para Adobe Flash Player

Números CVE: CVE-2015-3096, CVE-2015-3097, CVE-2015-3098, CVE-2015-3099, CVE-2015-3100, CVE-2015-3101, CVE-2015-3102, CVE-2015-3103, CVE-2015-3104, CVE-2015-3105, CVE-2015-3106, CVE-2015-3107 y CVE-2015-3108.

- **Fecha de Liberación:** 9-Jun-2015
- **Última Revisión:** 11-Jun-2015
- **Fuente:** Adobe Security Bulletin
- **Riesgo** Muy alto
- **Problema de Vulnerabilidad** Local
- **Tipo de Vulnerabilidad** Varios

1. Descripción

Adobe ha publicado actualizaciones de seguridad para Adobe Flash Player para sistema Windows, Linux y Macintosh. Estas actualizaciones corrigen vulnerabilidades que podrían permitir a un atacante tomar el control del sistema afectado. Adobe recomienda a los usuarios actualizar sus productos a las últimas versiones:

- ◆ Los usuarios de Adobe Flash Player Desktop Runtime para sistemas Windows y Macintosh deberían actualizar a Adobe Flash Player 18.0.0.160.
- ◆ Los usuarios de Adobe Flash Player Extended Support Release para sistemas Windows y Macintosh deberían actualizar a Adobe Flash Player 13.0.0.292.*
- ◆ Los usuarios de Adobe Flash Player para Linux deberían actualizar a Adobe Flash Player 11.2.202.466.
- ◆ Adobe Flash Player instalado con Google Chrome se actualizará automáticamente a la versión 18.0.0.160 (Windows y Linux) y 18.0.0.161 (Macintosh).
- ◆ Adobe Flash Player instalado con Internet Explorer en sistemas Windows 8.x se actualizará automáticamente a la versión 18.0.0.160.
- ◆ Los usuarios de Adobe AIR Desktop Runtime deberían actualizar a la versión 18.0.0.143 (Macintosh) and 18.0.0.144 (Windows).
- ◆ Los usuarios de Adobe AIR SDK y AIR SDK & Compiler deberían actualizar a la versión 18.0.0.143.

Versiones del software afectado

- ◆ Adobe Flash Player 17.0.0.188 y versiones anteriores para sistemas Windows y Macintosh.
- ◆ Adobe Flash Player Extended Support Release 13.0.0.289 y versiones anteriores a 13.x para sistemas Windows y Macintosh.
- ◆ Adobe Flash Player 11.2.202.460 y versiones anteriores a 11.x para sistemas Linux.
- ◆ Adobe AIR Desktop Runtime 17.0.0.172 y versiones anteriores para sistemas Windows y Macintosh.

- ◆ Adobe AIR SDK y SDK & Compiler 17.0.0.172 y versiones anteriores para sistemas Windows y Macintosh.
- ◆ Adobe AIR 17.0.0.144 y versiones anteriores para sistemas Android.

Para verificar la versión de Adobe Flash Player instalada en tu sistema, acceda a la [página About Flash Player](#) o ir al menú principal de la aplicación, dar clic en "Help" y seleccionar "About Adobe (o Macromedia) Flash Player". Si tú usas varios navegadores, realiza la comprobación para cada navegador que esté instalado en su sistema.

Para verificar la versión de Adobe AIR instalada en tu sistema, siga las instrucciones de Adobe AIR [TechNote](#).

2. Impacto

Adobe categoriza estas actualizaciones de acuerdo con las siguientes calificaciones prioritarias y recomienda a los usuarios actualizar la instalación de sus productos a la versión más reciente:

Producto	Versiones afectadas	Plataforma	Calificación de prioridad
Adobe Flash Player Desktop Runtime	17.0.0.188 y anteriores	Windows y Macintosh	1
Adobe Flash Player Extended Support Release	13.0.0.289 y anteriores	Windows y Macintosh	1
Adobe Flash Player para Google Chrome	17.0.0.188 y anteriores	Windows, Linux y Macintosh	1
Adobe Flash Player para Internet Explorer 10 e Internet Explorer 11	17.0.0.188 y anteriores	Windows 8.0 y 8.1	1
Adobe Flash Player	11.2.202.460 y anteriores	Linux	3
AIR Desktop Runtime	17.0.0.172 y anteriores	Windows y Macintosh	3
AIR SDK	17.0.0.172 y anteriores	Windows, Macintosh, Android y iOS	3
AIR SDK & Compiler	17.0.0.172 y anteriores	Windows, Macintosh, Android y iOS	3
AIR para Android	17.0.0.144 y anteriores	Android	3

Estas actualizaciones corrigen vulnerabilidades críticas en el software.

Detalles

Adobe ha publicado actualizaciones de seguridad para Adobe Flash Player para sistemas Windows, Linux y Macintosh. Estas actualizaciones corrigen vulnerabilidades que podrían permitir a un atacante tomar el control del sistema afectado. Adobe recomienda a los usuarios que actualicen sus productos a las versiones más recientes.

UNAM-CERT

- ◆ Los usuarios de Adobe Flash Player Desktop Runtime para sistemas Windows y Macintosh deberían actualizar a Adobe Flash Player 18.0.0.160.
- ◆ Los usuarios de Adobe Flash Player Extended Support Release para sistemas Windows y Macintosh deberían actualizar a Adobe Flash Player 13.0.0.292.
- ◆ Los usuarios de Adobe Flash Player para sistemas Linux deberían actualizar a Adobe Flash Player 11.2.202.466.
- ◆ Adobe Flash Player instalado con Google Chrome se actualizará automáticamente a la versión 18.0.0.160 (Windows y Linux) y 18.0.0.161 (Macintosh).
- ◆ Adobe Flash Player instalado con Internet Explorer en sistemas Windows 8.x se actualizará automáticamente a la versión 18.0.0.160.
- ◆ Los usuarios de Adobe AIR Desktop Runtime deberían actualizar a la versión 18.0.0.143 (Macintosh) y 18.0.0.144 (Windows).
- ◆ Los usuarios de Adobe AIR SDK y AIR SDK & Compiler deberían actualizar a la versión 18.0.0.143 (Macintosh) y 18.0.0.144 (Windows).
- ◆ Los usuarios de Adobe AIR para sistemas Android deberían actualizar a la versión 18.0.0.143.

Estas actualizaciones corrigen una vulnerabilidad (CVE-2015-3096) que podría ser explotada para evitar la corrección de la vulnerabilidad CVE-2014-5333.

Estas actualizaciones mejoran el direccionamiento de memoria aleatorio de Flash heap para plataformas Windows 7 de 64 bits (CVE-2015-3097).

Estas actualizaciones corrigen vulnerabilidades que podrían ser explotadas y conducir a divulgación de información (CVE-2015-3098, CVE-2015-3099 y CVE-2015-3102).

Estas actualizaciones corrigen una vulnerabilidad de desbordamiento de pila que podría provocar ejecución de código (CVE-2015-3100).

Estas actualizaciones corrigen un problema de permisos en Flash para Internet Explorer que podría ser explotado para escalar privilegios de bajo a medio nivel de integridad (CVE-2015-3101).

Estas actualizaciones corrigen una vulnerabilidad "Integer overflow" que podría provocar ejecución de código (CVE-2015-3104).

Estas actualizaciones corrigen una vulnerabilidad de corrupción de memoria que podría provocar ejecución de código (CVE-2015-3105).

Estas actualizaciones corrigen vulnerabilidades "Use-After-Free" que podrían provocar ejecución de código (CVE-2015-3103, CVE-2015-3106 y CVE-2015-3107).

Estas actualizaciones corrigen una vulnerabilidad "Memory leak" que podría ser usada para eludir ASLR - Address Space Layout Randomization (CVE-2015-3108).

Software afectado	Actualización recomendada	Disponibilidad
Flash Player Desktop Runtime	18.0.0.160	Flash Player Download Center Flash Player Distribution
Flash Player Extended Support Release	13.0.0.292	Extended Support

Flash Player para Linux	11.2.202.466	Flash Player Download Center
Flash Player para Google Chrome	18.0.0.160 (Windows y Linux) 18.0.0.161 (Macintosh)	Google Chrome Releases
Flash Player para Internet Explorer 10 e Internet Explorer 11	18.0.0.160	Microsoft Security Advisory
AIR Desktop Runtime	18.0.0.143 (Macintosh) 18.0.0.144 (Windows)	AIR Download Center
AIR SDK	18.0.0.143 (Macintosh) 18.0.0.144 (Windows)	AIR SDK Download
AIR SDK & Compiler	18.0.0.143 (Macintosh) 18.0.0.144 (Windows)	AIR SDK Download
AIR para Android	18.0.0.143	Google Play

3. Solución

Adobe recomienda a los usuarios actualizar su software instalado siguiendo las instrucciones a continuación:

- ◆ Adobe recomienda a los usuarios de Adobe Flash Player Desktop Runtime para sistemas Windows y Macintosh actualizar a Adobe Flash Player 18.0.0.160 visitando el [Centro de Descargas Adobe Flash Player](#) o mediante el mecanismo de actualización del producto cuando lo solicite.
- ◆ Adobe recomienda a los usuarios de Adobe Flash Player Extended Support Release actualizar a la versión 13.0.0.292 visitando <http://helpx.adobe.com/flash-player/kb/archived-flash-player-versions.html>.*
- ◆ Adobe recomienda a los usuarios de Adobe Flash Player para sistemas Linux la actualización a Adobe Flash Player 11.2.202.466 visitando el [Centro de Descargas Adobe Flash Player](#).
- ◆ Adobe Flash Player instalado con Google Chrome se actualizará automáticamente a la última versión de Google Chrome, la cual incluye Adobe Flash Player 18.0.0.160 (Windows y Linux) y 18.0.0.161 (Macintosh).
- ◆ Adobe Flash Player instalado con Internet Explorer para sistemas Windows 8.x se actualizará automáticamente a la última versión, la cual incluye Adobe Flash Player 18.0.0.160.
- ◆ Adobe recomienda a los usuarios de Adobe AIR Desktop Runtime actualizar a la versión 18.0.0.143 (Macintosh) y 18.0.0.144 (Windows) visitando el [Centro de Descargas Adobe AIR](#).
- ◆ Adobe recomienda a los usuarios de Adobe AIR SDK y AIR SDK & Compiler actualizar a la versión 18.0.0.143 (Macintosh) y 18.0.0.144 (Windows) visitando el [Centro de Descargas Adobe AIR](#).
- ◆ Adobe recomienda a los usuarios de Adobe AIR para sistemas Android actualizar a la versión 18.0.0.143 descargando la última versión desde la [tienda Google Play](#).

*Nota: A partir del 11 de agosto de 2015, Adobe actualizará la versión Extended Support Release de Flash Player 13 a Flash Player 18 para sistemas Windows y Macintosh. Para mantenerse al día con todas las actualizaciones de seguridad disponibles, los usuarios deben instalar la versión 18 de Flash Player Extended Support Release o actualizar a la versión más reciente disponible. Para más detalles, consulte esta entrada de [blog](#).

Agradecimientos

Adobe agradece a las siguientes personas y organizaciones por informar de los problemas pertinentes y por trabajar con Adobe para ayudar a proteger a nuestros clientes:

- ◆ Bilou, en colaboración con Chromium Vulnerability Reward Program (CVE-2015-3106)
- ◆ Chris Evans de Google Project Zero (CVE-2015-3097, CVE-2015-3104, CVE-2015-3105 y CVE-2015-3108)
- ◆ Haifei Li de McAfee Labs IPS Team (CVE-2015-3100)
- ◆ Pujun Li / PKAV team (pkav.net) (CVE-2015-3102)
- ◆ Malte Batram (CVE-2015-3098 y CVE-2015-3099)
- ◆ Natalie Silvanovich de Google Project Zero (CVE-2015-3107)
- ◆ Tomas Polesovsky (CVE-2015-3096)
- ◆ Wen Guanxing de Venustech ADLAB (CVE-2015-3103)

La Subdirección de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Jonathan Banfi Vázquez (jonathan dot banfi at cert 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