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

Boletin de Seguridad UNAM-CERT-2013-001 Vulnerabilidad de evasión del Gestor de Seguridad de Java 7

Existe una vulnerabilidad en la forma en que Java 7 restringe los permisos de aplicaciones que podría permitir a un atacante ejecutar comandos arbitrarios en un sistema vulnerable.

- **Fecha de Liberación:** 11-Ene-2013
- **Ultima Revisión:** 2-Abr-2013
- **Fuente:** http://www.kb.cert.org/vuls/id/625617
- **Riesgo** Alto
- **Problema de Vulnerabilidad** Local
- **Tipo de Vulnerabilidad** Ejecución de secuencia de comandos

1. Descripción

Una vulnerabilidad en el manejador de seguridad de Java permite a una aplicación de Java de otorgarse el permiso para ejecutar código arbitrario. Un atacante podría utilizar técnicas de ingeniería social para atraer a un usuario para que visite un un vínculo de un sitio web de alojamiento que contiene una aplicación de Java malicioso. Un atacante también podría comprometer un sitio web legítimo y subir un código malicioso de Java (un "drive-by download" ataque).

Cualquier navegador web utilizando el plug-in con la versión 7 de Java se verá afectado. El Java Deployment Toolkit plug-in y Java Web Start también se puede utilizar como vectores de ataques.

Los informes indican que esta vulnerabilidad está siendo activamente explotada, y el código del exploit está disponible públicamente.

Los detalles técnicos están disponibles en la Nota de Vulnerabilidad VU # 625617.

2. Impacto

Convenciendo a un usuario malicioso para cargar una aplicación de Java o Java Network Launching Protocol (JNLP) de archivos, un atacante podría ejecutar código arbitrario en un sistema vulnerable con los privilegios del Plug-inde Java.

3. Solución

Deshabilitar Java en los navegadores web.

Esta y las anteriores vulnerabilidades de Java han sido ampliamente dirigido por atacantes, y nuevas vulnerabilidades de Java podrían ser descubiertas. Para defenderse de esta y futuras vulnerabilidades de Java, desactivar Java en los navegadores web.
A partir de Java 7 Update 10, es posible deshabilitar Java contenido en los navegadores web a través del del panel de control de la aplicación de Java.

Ajuste el nivel de seguridad del cliente de Java:

Para instalaciones donde se requiere el mayor nivel de seguridad, es posible evitar totalmente cualquier aplicación de Java que se ejecute en un navegador seleccionando que no se ejecute el

contenido.

Si no puede actualizar a Java 7 version de actualización 10 consulte la sección de solución de la Nota de Vulnerabilidad VU # 636312 para obtener instrucciones sobre cómo desactivar Java en el navegador.

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

- Eric Bazzana (ebazzana 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