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

Boletin de Seguridad UNAM-CERT-2012-009 Vulnerabilidad de evasión del administrador de seguridad en Oracle Java 7

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

- **Fecha de Liberación:** 28-Ago-2012
- **Ultima Revisión:** 28-Ago-2012
- **Fuente:** CERT / CC
- **CVE ID:** TA12-240A
- **Problema de Vulnerabilidad** Local y remoto
- **Tipo de Vulnerabilidad** Puente de Seguridad

1. Sistemas afectados

Cualquier sistema usando Oracle Java 7 (1.7, 1.7.0) incluyendo:

- Java Platform Standard Edition 7 (Java SE 7)
- Java SE Development Kit (JDK 7)
- Java SE Runtime Environment (JRE 7)

2. Descripción

Una vulnerabilidad en el Java Security Manager podría permitir al applet de Java obtener permisos para ejecutar comandos arbitrarios en el sistema operativo. Un atacante podría utilizar técnicas de ingeniería social para hacer que usuarios visiten un enlace a un sitio web que aloje un applet malicioso.

3. Impacto

Tras convencer a un usuario para que cargue un applet malicioso de Java, un atacante podría ejecutar comandos arbitrarios del sistema operativo en un sistema vulnerable con los privilegios del proceso Java Plug-in.

4. Solución

Deshabilitar el Java Plug-in.

Deshabilitar el plug-in de Java del navegador web previene que los applets de Java sean ejecutados.

- Apple Safari: How to disable the Java web plug-in in Safari
- Mozilla Firefox: How to turn off Java applets
- Google Chrome: Ver la sección "Disable specific plug-ins" de la documentación de Plug-ins de Chrome.
- Microsoft Internet Explorer: El Panel de Control de Java (javacpl.exe) no utiliza la configuración de plug-in de Java para Internet Explorer. Es posible ejecutar javacpl.exe como Administrador, navegar a la pestaña Advanced, Default Java para navegadores, y utilizar la barra de espacio para quitar la selección de la opción de Microsoft Internet Explorer. Un método más directo es cambiar el valor de la llave de registro UseJava2IExplorer a 0. Dependiendo de las versiones de Windows y del plug-in de Java, las llaves pueden ser

encontradas en las siguientes ubicaciones:
HKLMSoftwareJavaSoftJava Plug-in{version}UseJava2IExplorer
HKLMSoftwareWow6432NodeJavaSoftJava Plug-in{version}UseJava2IExplorer

- Utilizar NoScript

NoScript es una extension de navegador para navegadores Mozilla Firefox que proporciona opciones para bloquear applets de Java.

5. Referencias

- http://www.us-cert.gov/cas/techalerts/TA12-240A.html
- Vulnerability Note VU#636312
- Zero-Day Season is Not Over Yet
- Let's start the week with a new Java 0-day in Metasploit
- http://pastie.org/4594319
- The Security Manager
- Java 7 0-Day vulnerability information and mitigation.
- How to disable the Java web plug-in in Safari
- How to turn off Java applets
- NoScript
- Vulnerability Summary for CVE-2012-4681

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

- Francisco Carlos Martínez Godínez (fmartinez at seguridad dot unam dot mx)
- Manuel Ignacio Quintero Martínez (mquintero 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