UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2008−029

Actualizaciones para múltiples vulnerabilidades en Sun Java

Sun ha generado alertas sobre multiples vulnerabilidades que afectan el Sun Java Runtime Environment. La mas severa de estas vulnerabilidades puede permitir a un atacante remoto ejecutar código arbitrario.

Fecha de Liberación: 5 de Diciembre de 2008

Ultima Revisión: 9 de Diciembre de 2008

Fuente: US−CERT

CVE ID: **TA08−340A**

Sistemas Afectados

Java	<=JDK and JRE 5.0 Update 17
Java	<=JDK and JRE 6 Update 11
Java	<=SDK and JRE 1.3.1_24
Java	<=SDK and JRE 1.4.2_19

Riesgo

Alto

Problema de Vulnerabilidad

Local y remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. **Descripción**

El Sun Java Runtime Environment (JRE) permite a los usuarios ejecutar aplicaciones Java en un navegador o en programas aislados. Sun ha liberado actualizaciones para el software de JRE para solucionar multiples vulnerabilidad.

Sun liberó las siguientes alertas referentes a estos problemas:

• 244986 : El Java Runtime Environment crea archives temporales que tienen nombres predecibles.

• 244987 : Java Runtime Environment (JRE) puede ser objeto de vulnerabilidades de Buffer Overflow al procesar archives de imágenes y estilos que usados en Applets o Java Web Start Applications permite la elevación de privilegios.

• 244988 : Múltiples vulnerabilidades en Java Web Start y Java Plug−in puede permitir la elevación de privilegios.

• 244989 : El mecanismo Java Runtime Environment (JRE) "Java Update" no verifica la firma digital de el JRE que descarga.

• 244990 : Una vulnerabilidad de Buffer Overflow en el Java Runtime Environment (JRE) puede permitir la elevación de privilegios.

• 244991 : Una vulnerabilidad de seguridad en el Java Runtime Environment (JRE) relacionada con Deserializing Calendar Objects (Objetos de deserialización de calendarios) puede permitir la elevación de privilegios.

• 245246 : El decodificador Java Runtime Environment UTF−8 puede permitir múltiples representaciones de las entredas en UTF−8.

• 246266 : Una vulnerabilidad de seguridad en el Java Runtime Environment puede permitir a los Applets listar el contenido del directorio inicial del usuario actual.

• 246286 : Existe una vulnerabilidad de seguridad en el Java Runtime Environment con el procesamiento de las llaves públicas RSA.

• 246346 : Una vulnerabilidad de seguridad en el Java Runtime Environment (JRE) con la autenticación de usuarios a través de Kerberos puede degenerar en una Denegación de Servicio (DoS)

• 246366 : Vulnerabilidades de seguridad en los paquetes JAX−WS y JAXB del Java Runtime Environment (JRE) puede permitir la elevación de privilegios.

• 246386 Una vulnerabilidad de seguridad en el Java Runtime Environment (JRE) con el análisis de archivos ZIP puede permitir leer ubicaciones de memoria arbitrarias.

• 246387 : Una vulnerabilidad de seguridad en el Java Runtime Environment (JRE) puede permitir a código leído desde el sistema de archivos local accesar al equipo local.

II. Impacto

El impacto de estas vulnerabilidades varia. La mas severa de estas vulnerabilidades permite a un atacante remote ejecutar código arbitrario

III. Solución

Aplicar las actualizaciones de Sun

Si se instalala la última version de Java, las versions anteriores pueden quedar instaladas. Si no son necesarias, deberían ser desinstaladas con las intrucciones que proporciona Sun en:

http://www.java.com/en/download/help/5000010800.xml

Deshabilitar Java

Deshabilitar Java en los navegadores web, como se describe en el documento Securing Your Web Browser :
http://www.us−cert.gov/reading_room/securing_browser/

Esto no arregla las vulnerabilidades descritas, sino bloquea un vector común de ataque.

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

- Manuel I. Quintero Martínez (mquintero at seguridad dot unam dot mx)
- Oscar Raúl Ortega Pacheco (oortega at seguridad dot unam dot mx)

UNAM−CERT
Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Cómputo
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