BOLETÍN DE ALERTA

Boletín Nro.: 2020-02

Fecha de publicación: 20/01/2020

Tema: Actualizaciones de seguridad críticas en Oracle Java SE

Las vulnerabilidades declaradas como críticas, son: CVE-2020-2601 - CVE-2020-2585 - CVE-2020-2593 - CVE-2020-2655 - CVE-2020-2654 - CVE-2020-2590 - CVE-2020-2659 - CVE-2020-2583

Sistemas afectados:

- Oracle Java SE, versiones 7u241, 8u231, 8u241, 11.0.5, 13.0.1.
- Oracle Java SE Embedded, versión 8u231.

Descripción:

Recientemente, Oracle publicó una colección de actualizaciones que solucionan múltiples fallos críticos de seguridad en sus productos.

Estos parches de seguridad, incluyen la solución a doce fallos en componentes de JAVA SE, que podrían ser explotados de manera remota y sin autenticación es decir, a través de una red sin necesidad de credenciales de usuario.

Los fallos se dan en los componentes **JavaFX, Serialization, Security, Networking, Libraries, JSSE**. Las mismas han sido catalogadas como: **Fáciles de explotar y Difíciles de explotar.**

Una de las vulnerabilidades difícil de explotar permite que un atacante no autenticado con acceso a la red a través de Kerberos comprometa Java SE, Java SE Embedded. Si bien la vulnerabilidad se encuentra en Java SE, Java SE Embedded, los ataques pueden afectar significativamente a productos adicionales. Los ataques exitosos de esta vulnerabilidad pueden resultar en acceso no autorizado a datos críticos o acceso completo a todos los datos accesibles. Esta vulnerabilidad se aplica a las implementaciones de Java, generalmente en clientes que ejecutan aplicaciones Java Web Start, que cargan y ejecutan código no confiable (por ejemplo, código que proviene de Internet), también puede explotarse mediante el uso de API en el componente especificado, por ejemplo, a través de un servicio web que suministra datos a las API.

Impacto:

Un atacante que logre explotar de manera exitosa estas vulnerabilidades podría proceder a la creación, eliminación o modificación no autorizada de los datos críticos de Java SE y/o causar un ataque de denegación de servicio parcial o total en Java SE.

Solución y Prevención:

Las actualizaciones que solucionan las vulnerabilidades, han sido publicadas por el fabricante, por lo que se recomienda aplicar las mismas lo antes posible.

Existen dos formas de aplicar estas actualizaciones:

- Desde el panel de control en Windows y OSx.
- Desde los navegadores Explorer, Firefox o Safari y Opera (Chrome no soporta Java desde su versión 42).

También es recomendable configurar las actualizaciones automáticas en Windows y en OSX. En el caso de no contar con las actualizaciones automáticas se recomienda:

1. Comprobar la versión de Java que tienes instalada desde el navegador. Ver aquí

Al aceptar y continuar, se comprobará la versión que tienes instalada y, si fuera necesario, recomendará la actualización más conveniente.

2. Actualizar directamente Java en tu ordenador a la última versión. Ver aquí
3. Para realizar otras acciones de seguridad relativas a Java, tales como eliminar versiones antiguas, configurar el nivel de seguridad o rechazar aplicaciones de origen desconocido, consultar estos consejos de seguridad. Ver aquí

Información adicional:

- https://www.oracle.com/security-alerts/cpujan2020.html
- https://www.oracle.com/security-alerts/cpujan2020verbose.html#JAVA