4.4.1. Artículo acerca del algoritmo de cifrado MD5 Raúl S. Moreno

El artículo nos comenta que la empresa Oracle ha anunciado que comenzará a bloquear los JAR que hayan sido firmados con el algoritmo de cifrado MD5. Este cambio se aplicará en la próxima versión de Oracle Java, la SE 8u131.

MD5 se considera un algoritmo muy básico que permite el cifrado de ficheros y datos en la base de datos, pero el problema surgió cuando se demostró que era inseguro y era posible llegar a dichos datos.

Si un usuario quiere comprobar la firma de su JAR lo puede realizar de forma sencilla con jarsinger, una aplicación cuyo ejemplo de uso es el siguiente:

"jarsigner -verify -J-Djava.security.debug=jar test.jar"

Dicha actualización de Java se considera una de las más importantes hasta la fecha ya que no solo englobará el problema con MD5 sino que agrupa soluciones a 270 vulnerabilidades.