Oracle lanza un nuevo parche de emergencia para Java

Ni Adobe ni Oracle están pasando por su mejor momento a nivel de seguridad. Y es que después de que gigantes como Facebook o Microsoft hayan sufrido ataques hacker en sus redes a través de una vulnerabilidad en el plug-in para navegadores de Java, los de Redwood Shores se han visto obligados a lanzar un nuevo parche de emergencia.

"**Estas vulnerabilidades son explotables remotamente sin autenticación**, es decir, pueden ser explotadas a través de una red sin la necesidad de utilizar nombre de usuario y contraseña", admite Oracle, que detectó el problema tan sólo unos días después de publicar su última actualización de seguridad en febrero.

"Para que un exploit tenga éxito, un usuario desprevenido que ejecute una de las versiones afectadas en su navegador debe visitar una página web maliciosa que aproveche esta vulnerabilidad", continúa. Lo graves es que "los exploits exitosos pueden afectar la disponibilidad, integridad y confidencialidad del sistema del usuario".

Además, las vulnerabilidades parcheadas en **JDK y JRE 7 Update 15, JDK y JRE 6 Update 41 y JDK y JRE 5.0 Update 40, y versiones anteriores** de las tres, estaban siendo empleadas para instalar un troyano de acceso remoto denominado **McRat**. Una vez dentro del equipo de la víctima, McRat se dedicaba (y se sigue dedicando) a copiarse a sí mismo en todos los archivos de sistemas Windows.

Debido a la gravedad de la situación, ya que el problema está siendo explotado activamente, Oracle recomienda encarecidamente a sus clientes que apliquen la nueva actualización de inmediato.