**Edward Jackson**

7/17/2015 1:19:16 PM

**Current event: Java Exploit, yet again**

Continuing to stay with the “security” theme, this week’s article is about Java and yet another exploit has been found. For everyone that does not know, Java is a programming language used in many web-based applications, especially security in web pages that use logon and authentication. Java will often times be installed and updated using a “plugin” update from Oracle. However, with this latest exploit, Oracle has yet to patch it. The exploit was observed in attacks against government ran organizations, such as NATO and the U.S. defense organizations. Basically, this unpatched exploit allows hackers to perform malvertising attacks, meaning, using the weakness in Java, hackers can launch their own malware-based attacks. This is particularly bad for the government because Java runs on many servers, of which if compromised, could bring down services being provided to government employees, the military, and other government staff members. The advice the article suggests is to just disable Java, but, I do not think that will be a good option for most government ran facilities, as many of their web services require the Java component. Really, it is just bad all the way around. These hackers, which some think are from Russia, are committing cyberespionage. I believe there is a solution, and that is for the government to get involved with testing Java, as well as tracking down these hackers. It really is a scary thought, because cyber-attacks, cyberespionage, and cybercrime in general are on the rise.

References

Constantin. (2015). Cyberespionage group Pawn Storm uses exploit for unpatched Java flaw. Retrieved from http://www.computerworld.com/article/2947216/security/cyberespionage-group-pawn-storm-uses-exploit-for-unpatched-java-flaw.html