DMZ Gateway version 3.x uses Java 1.6.0 build 14. Is there any concern over known remote vulnerabilities in this version of Java?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- DMZ Gateway, version 3.0

QUESTION

DMZ Gateway version 3.0 uses Java 1.6.0 build 14. Is there any concern over known remote vulnerabilities in this version of Java?

ANSWER

Communication between EFT and DMZ Gateway is via standard sockets and relies on a proprietary protocol; therefore, we currently do not have any known vulnerabilities as a result of using a JVM to run our application.

With each build of DMZ Gateway, the Java Runtime Environment is updated to the latest release. DMZ Gateway v3.1.1 uses the JRE v1.6.0_24; version 3.2.0 uses the JRE v1.4.0; version 3.4.0 uses the JRE v1.8.0_74.

Java vulnerabilities are often very confusing as they can exist with JavaScript (which isn't truly Java, but often creates said confusion), Java Applets (which is Java, but runs within a sandbox on remote computers), or via Java Communication APIs (which can be RMI, JNI, etc). GlobalSCAPE uses the Java Virtual Machine (JVM) to build software that can be run across multiple architectures, but does not rely on any of the aforementioned features that likely contain the security vulnerabilities addressed in subsequent builds of the Java Virtual Machine.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/10646/DMZ-Gateway-version-3x-uses-...