Harnett County IT Dept

Monthly Security Tips NEWSLETTER

August 2013 Volume 8, Issue 8

Java Exploits

What is Java?
Java is a computer language that allows programmers and application developers to write software that can run on many different operating systems. Many applications and websites require end-users to have Java installed. Websites incorporate Java applets (small applications) to enhance the usability and functionality of a website. In general, when a user visits one of these websites, depending on their browser's security settings, they may have no idea that the Java applet is automatically running.

End-users typically have "Java Runtime Environment" (JRE) installed on their computer. In many instances, this software was pre-installed on their computer. More recently, this practice is becoming less common. If JRE is not installed on your computer, and you visit a website that requires JRE, generally, you will be prompted to install JRE.

What are the Risks with Java?
Java is designed to work on almost any computer. Java has been prone to numerous reports of vulnerabilities. Cyber criminals can create a single attack tool that can potentially hack almost any computer in the world. According to the SecureList IT Threat Evolution Report released by Kaspersky Lab in May 2013, "The most widespread vulnerabilities are found in Java and [the vulnerabilities] were detected on 45% of all computers." [1]

These attacks are based, at least in part, on older versions of Java. When a newer version of Java is released and installed on a machine, the older version may not automatically be uninstalled. This was intended to provide an easy way to roll back to an older version in case of compatibility issues. Attacks can be used by hackers to leverage and to exploit the vulnerabilities that exist in those versions. This makes Java's weaknesses an attractive target for hackers and cyber criminals.

How Can I Mitigate Java Exploits?

- Enable the automatic update feature, which will ensure you receive important security updates when they are released. Visit: http://www.java.com/en/download/help/java_update.xml for instructions on turning on the auto-update feature.

- Set the Java security level to "High" or "Very High". The most recent versions of Java have the ability to manage when and how untrusted Java applications/applets will run. You can set the security level from within the Java Control Panel so that you are notified before any untrusted Java applications run. Visit: http://www.java.com/en/download/help/jcp_security.xml for instructions on setting the Java security level.

- Clear the Java cache periodically. This forces the browser to load the latest versions of web pages and programs. For more information visit: http://www.java.com/en/download/help/plugin_cache.xml

[1] http://www.securelist.com/en/analysis/204792292/IT_Threat_Evolution_Q1_2013

- Do not allow applications from unknown publishers to run.

- Remove older, unneeded Java versions. If a certain version of Java is needed, determine what Java release level is needed and remove all versions prior to that. For more information visit: http://www.java.com/en/download/faq/remove_olderversions.xml

For More Information:

For additional information, please visit:

What is Java?
https://en.wikipedia.org/wiki/Java_(programming_language)

Java Security Resources
http://www.java.com/en/security/

Uninstalling Java on Windows
http://www.java.com/en/download/uninstall.jsp

Uninstalling Java on Mac
https://www.java.com/en/download/help/mac_uninstall_java.xml

Disabling Your Browser's Java Plugin
https://krebsonsecurity.com/how-to-unplug-java-from-the-browser/

Brought to you by:

CENTER FOR INTERNET SECURITY®

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

STOP | THINK | CONNECT™