State of Illinois
Central Management Services
Monthly Cyber Security Tips
NEWSLETTER

December 2010 Volume 5, Issue 12

Increase in Java Exploits

Java is a programming and computing platform widely used for stand-alone and web-based applications/applets, including utilities, games, and business applications. The platform was first released by Sun Microsystems in 1995. Many applications and websites require end-users to have Java installed, and the software is used extensively because of its flexibility. Once a program has been created and compiled in Java, it will run on a variety of software and operating system platforms (such as Windows and Macs).

What are the potential cyber security concerns?
There has been a rapid increase in the amount of malware that attempts to exploit vulnerabilities in Java. In the second quarter of 2010, there were an estimated 500,000 exploits, up from virtually zero a year before. Between Q2 2010 and the middle of Q3, that figure had increased to more than six million.[1]

The attacks are based in part on older versions of Java. When a newer version of Java is released and installed on a machine, the older version does not automatically get uninstalled. This behavior was intended to provide an easy way to roll back to an older version in case of compatibility issues. However, there is an exploit code publically available on the Internet that hackers are using which detects whether previous versions of Java are installed on a user's machine and exploits the vulnerabilities that exist in those versions.

What can I do to be safe?
It is important that users are installing the latest version of Java released by Oracle. To confirm the correct version, visit the following site: http://www.java.com/en/download/installed.jsp.

Because older versions of Java are not automatically removed when newer versions are installed, it is recommended that users take the extra step of uninstalling the older versions if they are not needed. The uninstallation can be accomplished by using an application known as ***JavaRa,*** which is designed to remove all traces of older Java installations on your system.

Home users typically do not need the older versions of Java installed once they have upgraded their Java software and should follow the steps below to remove the older versions of Java.

To remove Java software using the JavaRa tool:

- Download the tool from: http://raproducts.org/wordpress/software
- Once this tool is downloaded, perform the following steps:
- Double click on JavaRa.zip
- Locate the file named JavaRa.exe
- When prompted whether or not you want to allow the program to run, click run.

[1] http://www.zdnet.co.uk/blogs/security-bullet-in-10000166/microsoft-warns-of-java-exploit-rise-10020826/

- From the drop down box, select your language and click on the Select button.
- Now that the program is running, you can Search for Java Updates or Remove Older Versions of Java.

Please note that the Multi-State Information Sharing and Analysis Center (MS-ISAC), a division of the Center for Internet Security, makes no warranties, express or implied, as to the safety and reliability of the JavaRa application.

We encourage enterprise users to check with their respective Information Technology (IT) Department and Information Security Office (ISO) prior to downloading, installing, and using this or any product. Additionally, always ensure that your anti-virus and anti-spyware products are up-to-date.

For More Information:

Microsoft:
http://blogs.technet.com/b/mmpc/archive/2010/10/18/have-you-checked-the-java.aspx

JavaRa:
http://raproducts.org/wordpress/software
http://raproducts.org/javara.html

ZDNet:
http://www.zdnet.co.uk/blogs/security-bullet-in-10000166/microsoft-warns-of-java-exploit-rise-10020826/

Techworld:
http://news.techworld.com/security/3246147/mac-users-hit-with-windows-style-koobface-trojan/

Cisco:
http://blogs.cisco.com/security/java-exploits-another-example-of-tomorrows-threat-landscape-today-2/

SANS Internet Storm Center:
http://isc.sans.edu/diary.html?storyid=9916

For more monthly cyber security newsletter tips visit: www.msisac.org/awareness/news/

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. Organizations have permission--and in fact are encouraged--to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by:

The MS-ISAC, a Division of the Center for Internet Security
www.msisac.org