Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

July 2013

Java Vulnerability Mitigation

Guidance for the Government of Canada

ITSB-98

Introduction

Java is a programming language and computing platform used by a multitude of authorized systems and business processes and has an installation base of nearly one billion. Over the past year, cyber-intruders have discovered and exploited a number of Java vulnerabilities; some of which are able to compromise the security of the Department's network holdings without warning. The delay between the discovery of a vulnerability and the design and implementation of a mitigation patch facilitates the exploitation potential of that vulnerability by cyber-intruders. Consequently, a Department's network could remain vulnerable for an extended period of time.

Target Audience

This bulletin is intended for information security practitioners responsible for IT security risk management activities and is structured to be used within the framework of Information Technology Security (ITS) management activities defined within the publication: CSEC - IT Security Risk Management: A Lifecycle Approach (ITSG-33).

Vulnerability

In January of 2013, knowledge of an exploit that targeted vulnerabilities in Oracle's Java software was made public[1]. The vulnerability was found in both the Java Development Kit (JDK) and the Java Runtime Environment (JRE), deployed on most business and personal computers. This zero-day exploit was leveraged by convincing users to browse a malicious website with their Java enabled browser. Once connected to the infected site a malicious Java program would run, by-passing security checks, allowing the remote agent to gain full administrative access to the users' computer. Although a fix for this problem was quickly released, another zero-day exploit was rapidly created to circumvent the fix.

Various versions of Java can be used and exploited in different ways; for example Java can be accessed via a web browser or it can be host based. When the numbers of different Java capable web browsers are factored in it becomes clear that the attack surface is significant. Each Department's ITS Threat and Risk Assessment (TRA) should be revised to consider existent Java vulnerabilities and to include an updated assessment of the residual risk to the Department's network holdings.

Impact on the Government of Canada (GC)

The GC has thousands of systems installed with the Java platform and Departments have relied on both host based and browser based Java applications to perform valid business processes. In most circumstances, the systems that utilize these Java applications execute on networks with internet access. This can be problematic if Java is plugged into the default browser and the user connects to a malicious website. The computer can then be exploited through vulnerabilities in the Java plugin and expose the department's network holdings to unauthorized users.

Recommended Mitigation Measures

The following options for mitigating Java exploits are recommended:

1 Specifically exploit CVE-2013-0422 targeted Java 7 Update 10 and earlier; previous Java versions were not affected.

1. Install Patches

The CSEC Top 35 Mitigation Measures, ITSB-89A, lists patch maintenance as the #2 mitigation measure. System administrators should immediately ensure that the most up to date patches have been applied to their Java products.

2. Un-Install Java

If Java is not required for the normal operations of departmental business it should be un-installed. This measure will protect the IT assets from current and future exploits.

3. Restrict Java-Enabled Browsing to a Virtual Environment

Java enabled browsing that is sandboxed within a virtualized operating system help ensure that the corruption of that environment through a Java exploit has a minimal impact on the physical system, especially if the virtual environment is non-persistent and returns to a known secure configuration after use or restart.

4. Disable Java Browser Plugin

The Java plug-in can be disabled in all browsers if it is not required for an essential departmental function.

5. Disable Java in the Default Browser

This option assumes that a web based Java program must be utilized in the Department on a regular basis. It requires that users employ two browsers: one for limited internet browsing for instances when Java is required and one for all other internet access. Java should be disabled in the default browser so that if the default browser is started by malicious code, the Java program would not be readily available. If Java is required, then the alternative web browser (with Java enabled) could be used. It should be noted that the success of this option requires careful compliance on the part of the end users or to proxy the Java enabled browser to limit its use to safe web sites.

6. Restrict Access to Java at the Firewall

This option allows the Department to continue to use Java internally, as well as on selected websites, while mitigating vulnerabilities by restricting access to Java on prohibited sites. This can be done using proxy server rules to help control to use of Java. For example:

- Whitelisting[2] essential web sites that use Java and blocking all others;
- Filtering requests that contain a Java User-Agent header to allow Java to be used on the Department's network while blocking all other requests; and
- Blocking outgoing traffic with jar, cla, class, jnlp, jardiff and java extensions.

Summary

While Java is a useful business tool, it has also become the focus of the cyber-intruder community who continue to expose and exploit its vulnerabilities. These vulnerabilities can undermine the security of the GC's networks.

It is recommended that Departments avoid reliance on products which require Java to function; especially when it requires the installation of Java on a user's desktop where web browsing or e-mail activity will be conducted. Where possible, the preferred mitigation measure is the removal of Java from the Department's network.

Additional Information

For additional IT security advice and guidance, contact: itsclientservices@cse-cst.gc.ca.

2 A 'Whitelist' is a register of websites with a presumed trusted relationship and privileged to use Java.