the Availability Digest

www.availabilitydigest.com

Department of Homeland Security Says, “Disable Java”

January 2013

The Computer Emergency Readiness Team (CERT) of the U.S. Department of Homeland Security (DHS) has issued an alert urging computer users to disable Java in their browsers. This unprecedented action followed the discovery of a serious Java vulnerability that allows hackers to infect PCs with malicious code. The vulnerability has existed undetected for some time.

Java is a language used by hundreds of millions of computers worldwide to access interactive content and web applications. Oracle Corp. purchased Java as part of its U.S. $7.3 billion acquisition of Sun Microsystems in 2010.

The Announcement

On Thursday, January 10, 2013, the DHS issued US-CERT Alert TA13-010A, Oracle Java 7 Security Manager Bypass Vulnerability.[1] This security hole in Java 7 allows hackers to install malicious code for key logging; for stealing sensitive personal information such as credit card numbers, social security numbers, and bank account numbers; and for other cyber criminal actions.

The vulnerability is being actively exploited. Explicit code is available in “exploit kits,” which are prepackaged, for-sale toolkits that can be used to install malicious code. Infection is generally accomplished by attracting victims to infected web sites.

Windows, MAC OS, and Linux systems are all affected. The risks include all versions of Java 7 through Update 11 and the following Java systems:

Java Platform Standard Edition 7 (Java SE 7)
Java SE Development Kit (JDK 7)
Java SE Runtime Environment (JRE 7)
Web browsers using Java 7 plug-ins

Earlier versions of Java, from Java 6 and before, are unaffected.

The Vulnerability

The vulnerability is caused by a weakness in the way Java 7 restricts permissions of Java applets. It allows a Java applet to grant itself permission to execute arbitrary code. By using this vulnerability, an untrusted Java applet can escalate its privileges without requiring code signing. Unprivileged Java code then can have unrestrained access to restricted classes. As a result, an attacker can execute any commands it chooses on a vulnerable system.

[1] http://www.us-cert.gov/cas/techalerts/TA13-010A.html

Attackers employ social engineering techniques to entice a user to visit an infected web site hosting a malicious Java applet. Alternatively, the attacker can infect a legitimate site with a malicious applet. In either case, the applet is downloaded to the PC in an HTML document, infects the PC, and opens it to the attacker's actions.

Any browser using the Java 7 plug-in is affected. In addition, the Java Development Toolkit plug-in and Java Web Start also can be attack vectors.

Further details on this vulnerability can be found in CERT's Vulnerability Note VU#625617, Java 7 fails to restrict access to privileged code.[2]

Recommended Actions

The DHS's recommendation to fix this problem is simple – disable Java 7.

Starting with Java 7 Update 10 (J7u10), it is straightforward to disable Java content in web browsers through the Java control applet. However, earlier versions of Java do not provide such an obvious disabling mechanism. The DHS Alert referenced above and CERT's Vulnerability Note 636312, Oracle Java JRE 1.7 Expression.execute() and SunToolkit.getField() fail to restrict access to privileged code,[3] provide guidance for disabling earlier versions of Java.

Java 7 Update 11 (J7u11) has been enhanced to set the default Java security settings to "High" so that users will be prompted before running unsigned or self-signed Java applets. Furthermore, on Sunday, January 13th, three days after the DHS alert, Oracle released an emergency update to correct the problem. However, even with these fixes, CERT continued to recommend disabling Java. Its Vulnerability Note 625617 contains the following advice:

> "Unless it is absolutely necessary to run Java in web browsers, disable it as described below, even after updating to 7u11. This will help mitigate other Java vulnerabilities that may be discovered in the future."

In fact, vulnerabilities do continue to be discovered. Several security firms have already discovered additional vulnerabilities in Java 7 Update 11 that can be exploited to bypass Java's security sandbox and execute arbitrary code on computers. Working proof-of-concept exploit code has been provided to Oracle as late as the end of January.

Security experts have been advising for some time to disable Java since it is so commonly targeted by cyber criminals. Most platforms do not come with Java, and by and large the common activities upon which computer users depend do not use Java. Thus, disabling Java should have little effect if any on the average user.

Some computer vendors are being proactive in attacking this problem. Last fall, Apple issued a MAC OS update that prevents Java from running in its browsers at all. On Friday, January 11th, the day following the DHS alert, Mozilla announced it was blocking all recent Java programs from automatically loading in its Firefox browser unless a user specifically allows it.

[2] http://www.kb.cert.org/vuls/id/625617

[3] http://www.kb.cert.org/vuls/id/636312

Summary

According to security software maker Kaspersky Labs, Java is the most frequently attacked piece of software and accounted for 50% of all cyber attacks in 2012. Kaspersky Labs is the Russian security company that discovered the devastating Stuxnet virus.[4]

Security experts say that Oracle's Java 7 problem was caused by "an incomplete patch developers issued last year to fix an earlier (similar) security bug" (see CERT's Vulnerability Note VU#636312 referenced above).

Rarely does a government agency recommend the disabling of software. This action clearly indicates the severity of the vulnerability. Even worse, DHS says that it is currently unaware of a practical solution to the problem.

Acknowledgements

Material for this article was taken from the following sources:

Oracle Java 7 Security Manager Bypass Vulnerability, *US-CERT Alert TA13-010A*; January 10, 2013.
Java 7 fails to restrict access to privileged code, *Vulnerability Note VU#625617*; January 10, 2013.
Oracle Java JRE 1.7 Expression.execute() and SunToolkit.getField() fail to restrict access to privileged code, *Vulnerability Note VU#636312*; August 27, 2012.
US Department of Homeland Security Calls on Computer Users to Disable Java, *Forbes*; January 11, 2013.
Department of Homeland Security advises computer users to disable Java because of security bug, *Yahoo.com*; January 12, 2013.
U.S. Government to PC Users: Disable Java, *Newsy*; January 12, 2013.
US department of Homeland Security advises disabling Java following fresh zero-day vulnerability, *The Verge*; January 13, 2013.
US homeland security warns computer users to disable Java software due to security threat, *Independent.ie*, January 14, 2013.
Researchers find critical vulnerabilities in Java 7 Update 11, *Computerworld*; January 18, 2013.
Latest Java Flaw Bypasses Security Control, Security Researchers Say, *eWeek*; January 28, 2013.

[4] Stuxnet – The World's First Cyberweapon, *Availability Digest*; March 2011.
http://www.availabilitydigest.com/public_articles/0603/stuxnet.pdf