the Availability Digest

www.availabilitydigest.com

Oracle Releases Massive Security Patch for Java

May 2013

Following last January's recommendation by the U.S. Department of Homeland Security (DHS) to disable Java in browsers,[1] Oracle now has come out with a massive set of patches to try to plug Java security holes. These patches have been released in Oracle's April 2013 Critical Patch Update (CPU) for Java SE. The release is an attempt to halt ongoing hacker attacks using the Java programming language that runs inside browsers

April 2013 Critical Patch Update for Java SE

Oracle releases CPUs every quarter, with special patch releases provided more frequently if critical vulnerabilities are found. On April 16th, Oracle released its April 2013 Critical Patch Update for Java SE. Affected Java versions include Java 5 (Update 41) and earlier, Java 6 (Update 43) and earlier, and Java 7 (Update 17) and earlier. The release comes a few months after Facebook, Twitter, and NBC News suffered attacks that allowed hackers to infiltrate their internal networks through Java vulnerabilities

The April 2013 CPU for Java SE addresses forty-two security flaws. Thirty-nine vulnerabilities were remotely exploitable without authentication (username and password). These vulnerabilities would have allowed a remote, unauthenticated attacker to execute arbitrary code, to cause a denial-of-service, or to gain unauthorized access to a company's files or systems.

Nineteen of these vulnerabilities carried a CVSS score of ten. CVSS (Common Vulnerability Scoring System) is a widely used standard for rating security vulnerabilities. It considers how easy it is to launch an attack and the impact of a successful attack using a vulnerability. The highest CVSS score is ten. A value of ten indicates that an easy, over-the-network, unauthenticated takeover of the operating system can be made.

Thus, almost half of the vulnerabilities that were patched by the April 2013 CPU for Java SE were as bad as they get. One of the biggest changes with the April patch update is that websites will no longer be able to force unsigned Java applets to run. Users, however, can override the default setting by acknowledging the risk.

The April 2013 patches address vulnerabilities that were found during this year's Pwn2Own competition. Pwn2Own is a computer-hacking contest held annually at the CanSecWest Security Conference. Contestants are challenged to exploit widely used software and mobile devices with previously unknown vulnerabilities

[1] Department of Homeland Security Says, "Disable Java", *Availability Digest*; January 2013. http://www.availabilitydigest.com/public_articles/0801/disable-java.pdf

During this year's contest held in March in Vancouver, Canada, three hackers successfully attacked Java. One hacker circumvented Java's Address Space Layout Representation (ASLR) and its Data Execution Prevention (DEP) to take control within 15 seconds of a fully patched Windows OS.

Java has now surpassed Adobe Reader as the most frequently attacked piece of software. In 2011, Adobe Reader accounted for 35% of attacks compared to Java's 25%. In 2012, 50% of the attacks were made against Java as compared to 28% made against Adobe Reader.

April 2013 Critical Patch Update

On the same day that it released its Java SE patch, Oracle also released its April 2013 Critical Patch Update, which applied 128 patches to thirteen of its product suites. Patched products included the Oracle Database, Oracle Fusion Middleware, Oracle E-Business Suite, Oracle Supply Chain Products Suite, Oracle PeopleSoft Enterprise, Oracle Siebel CRM, Oracle FLEXCUBE, Oracle Industry Applications, Oracle Primavera, Oracle and Sun Systems Product Suite, Oracle MySQL, and Oracle Support Tools.

Several of these patches had CVSS scores of ten. Four addressed Oracle database security vulnerabilities that could be exploited remotely without a user name or password.

Summary

The Java ecosystem pioneered many new features that made developing software for multiple platforms easier. The Java Runtime Environment was the result of that need for easier cross-platform development. Sadly, the reputation of the Java ecosystem has taken a significant hit due to the large number of security vulnerabilities exposed in the JRE and in Oracle's software-development lifecycle.

As H. D. Moore, chief security officer at Rapid 7 explains,[2] "The Java sandbox was designed when the threat to desktop users was very different. The current generation of sandboxes (Chrome, Adobe, IE) are implemented one level higher -- restricting what the sandboxed process can do and not trying to enforce all of the logic within the runtime itself. Java's sandbox is still of the older variety. All it takes is one logic flaw to go from a webpage to running code in the context of the user."

Nevertheless, if you are committed to Java, as many companies are, the number of patches in the April 2013 CPUs can seem overwhelming. Experts suggest that you patch the Internet-exposed services first. Then consider the highest severity patches – those with a CVSS score of ten, followed by patches of lessor severity.

Acknowledgements

Material for this article was taken from the following resources:

How to secure Java amid growing Java security vulnerabilities, *Search Security*; undated.
Oracle issues out-of-band patch to repair 50 Java vulnerabilities, *Search Security*; February 4, 2013.
Accuvant Labs Releases Pwn2Own-Winning Java Exploit Details, *Business Wire*; undated.
Oracle to release 128 security patches, hundreds of products affected, *ZDNet*; April 16, 2013.
April 2013 Critical Patch Update for Java SE Released, *Oracle Blog*; April 16, 2013.
April 2013 Critical Patch Update, *Oracle Blog*; April 16, 2013.
Oracle releases mega security patch for Java, *Computer Weekly*; April 17, 2013.
Oracle Fixed 128 Vulnerabilities with April 2013 CPU, *Softpedia*; April 17, 2013.
Oracle Has Released Multiple Updates for Java SE, *US-CERT*; April 19, 2013
Oracle Java Critical Patch Update April 2013 Review, *Eric Romang Blog*; undated.

[2] Java vulnerabilities continue to crop up with Java 7, Update 11 release, *Search Security*; January 21, 2013.