Security Vulnerability Notice

SE-2012-01-IBM-3

[Security vulnerabilities in Java SE, Issues 70-71]

DISCLAIMER

INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW NEITHER SECURITY EXPLORATIONS, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE INFORMATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS, OR OTHER RIGHTS. THERE IS NO WARRANTY BY SECURITY EXPLORATIONS OR BY ANY OTHER PARTY THAT THE INFORMATION CONTAINED IN THE THIS DOCUMENT WILL MEET YOUR REQUIREMENTS OR THAT IT WILL BE ERROR-FREE.

YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION AND USE OF THE INFORMATION TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE, AND RESULTS OBTAINED FROM IT.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL SECURITY EXPLORATIONS, ITS EMPLOYEES OR LICENSORS OR AFFILIATES BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA, OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION, OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE, OR OTHER THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE INFORMATION CONTAINED IN THIS DOCUMENT, EVEN IF SECURITY EXPLORATIONS OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS.

Security Explorations discovered two additional security issues in the latest version of IBM SDK, Java Technology Edition software [1]. A table below, presents their technical summary:

ISSUE #	TECHNICAL DETAILS	
70	origin	com.ibm.rmi.io.SunSerializableFactory
	cause	arbitrary class deserialization in a privileged code block
	impact	creation of custom and fully functional java.lang.ClassLoader objects
	type	complete security bypass vulnerability
71	origin	com.ibm.rmi.corba.ProxyStub
	cause	insecure use of invoke method of java.lang.reflect.Method class
	impact	arbitrary method invocation inside AccessController's doPrivileged block
	type	complete security bypass vulnerability

Below, we provide additional comments with respect to the reported issues:

- Issue 70 allows to create custom instances of Serializable classes inside AccessController's doPrivileged block. During instance creation, a constructor of the first non-serializable superclass is called. This allows for a creation of fully functional instances of java.lang.ClassLoader class. That condition alone is sufficient [2] to define arbitrary classes in a privileged ProtectionDomain.
- Issues 71 is yet another instance of insecure use of invoke method of java.lang.reflect.Method class inside AccessController's doPrivileged block. It is similar to previously reported Issues such as 33, 34 and 67. The difference is that this time only instance methods can be abused. This is not an obstacle at all. In our Proof of Concept code, we make use of the exploitation scenario presented for Issue 68 (privileged access to protectionDomain field of java.lang.Class).

Additionally, we would like to point out that Issue 49 (originally reported to IBM in Sep 2012) is still not fixed properly. The patch for it (the second attempt to address it) can be still bypassed. As a result, arbitrary classes can be defined in a privileged classloader namespace.

Attached to this report, there are 3 Proof of Concept codes that illustrate both new vulnerabilities and the improper patch for Issue 49. Each of them demonstrates a complete compromise of a Java security sandbox. They have been successfully tested in a 32-bit Linux OS environment and with the following version of IBM SDK:

- IBM SDK, Java Technology Edition, Version 7.0 SR5 for Linux (32-bit x86), build pxi3270sr5-20130619_01(SR5)

REFERENCES

[1] IBM developer kits , http://www.ibm.com/developerworks/java/jdk/

[2] Calendar Bug, (Slightly) Random Broken Thoughts, Sami Koivu , http://slightlyrandombrokenthoughts.blogspot.com/2008/12/calendar-

bug.html

About Security Explorations

Security Explorations (http://www.security-explorations.com) is a security start-up company from Poland, providing various services in the area of security and vulnerability research. The company came to life in a result of a true passion of its founder for breaking security of things and analyzing software for security defects. Adam Gowdiak is the company's founder and its CEO. Adam is an experienced Java Virtual Machine hacker, with over 50 security issues uncovered in the Java technology over the recent years. He is also the hacking contest co-winner and the man who has put Microsoft Windows to its knees (vide MS03-026). He was also the first one to present successful and widespread attack against mobile Java platform in 2004.