Security Vulnerability Notice

SE-2012-01-ORACLE-4

[Security vulnerabilities in Java SE, Issues 27-31]

DISLAIMER

Security Explorations discovered additional security issues in Java Platform, Standard Edition and related technologies such as JavaFX in particular. All weaknesses are similar to those discussed in our previous reports (problems with Reflection API). A table below, presents their technical summary:

ISSUE #	TECHNICAL DETAILS	
27	origin	`sun.plugin2.applet.JNLP2ClassLoader` class
	cause	no security check upon loading of a class from a restricted package
	impact	arbitrary access to restricted classes (JavaFX environment only)
	type	partial security bypass vulnerability
28	origin	`com.sun.beans.finder.FieldFinder` class
	cause	insecure use of `getFields` method of `java.lang.Class` class
	impact	access to field objects from restricted classes and interfaces
	type	partial security bypass vulnerability
29	origin	`java.lang.reflect.Proxy` class
	cause	no security check for restricted interfaces
	impact	the ability to create fully functional Proxy objects for interfaces belonging to restricted packages
	type	exploitation vector (requires a security bypass precondition)
30	origin	`com.sun.corba.se.impl.orbutil.GetPropertyAction` class
	cause	public class
	impact	arbitrary access to Java system properties
	type	partial security bypass vulnerability
31	origin	`sun.misc.Service` class
	cause	lack of a type check of a script engine class prior to creating its instance
	impact	the ability to bypass security checks implemented in static class initializers of a 3rd party software
	type	partial security bypass vulnerability

Below, we provide additional comments with respect to the issues presented in the table above:

- Issue 27 was tested in the environment of Java SE 7 with JavaFX running atop. It only affects JavaFX applications (in Java Web Start, there is a proper call to `checkPackageAccess` method of a current `SecurityManager` object). The issues were verified to be present both in the latest JavaFX 2.0.3 and early access 2.2.0 runtimes.
- Issue 29 is presented as an exploit vector for Issues 27 and 28 in the Java SE 7 environment. The exploitation vector allows for the creation of arbitrary Proxy objects for interfaces defined in restricted packages. In our Proof of Concept code we create such a proxy object for the `com.sun.xml.internal.bind.v2.model.nav.Navigator` interface. In order to use the aforementioned proxy object, we need an instance of that interface too. We obtain it with the help of Issue 28, which allows to access arbitrary field objects from restricted classes and interfaces. As a result, by combining Issue 27-29, one can use `Navigator` interface and make use of its sensitive Reflection API functionality to achieve a complete JVM security bypass condition.

- Issue 30 is similar to Issue 14 (arbitrary access to Java system properties). Same for Issue 31, which is almost the same as Issue 15. Issue 31 is however not limited to system class loader namespace.

Attached to this report, there are several Proof of Concept codes that illustrates all reported vulnerabilities. They have been successfully tested in a Windows environment and with the latest versions of Java SE 6 (Issues 30-31) and JavaFX running atop of Java SE 7 (Issue 27-29).

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.