

# Security Vulnerability Notice

SE-2014-01-ORACLE-2

[Security vulnerabilities in Oracle Database Java VM, Issues 21-22]

## 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 additional 2 security vulnerabilities in the implementation of a Java VM embedded by Oracle Database software. These new vulnerabilities are also the result of insecure implementation of Java Reflection API. Their successful exploitation can easily lead to the full compromise of a Java security sandbox of a target database server instance. This can further be exploited to execute arbitrary OS commands on a database server or to gain administrator privileges in a target Oracle Database.

A table below presents a summary of reported Java security issues:

ISSUE #	TECHNICAL DETAILS	
21	origin	<code>oracle.jdbc.OracleConnectionWrapper\$CloseInvocationHandler</code>
	cause	insecure use of <code>invoke</code> method of <code>java.lang.reflect.Method</code> class
	impact	arbitrary static method invocation
	type	partial security bypass vulnerability
22	origin	<code>oracle.aurora.util.JRIExtensions</code>
	cause	insecure use of <code>getMethods()</code> method of <code>java.lang.Class</code> class
	impact	access to methods of arbitrary classes
	type	partial security bypass vulnerability

Attached to this report, there is a Proof of Concept code module (`POC9.java`) illustrating discovered weaknesses. It was successfully verified in the environment of the most recent Oracle Database 12c software (Oracle Database 12c Release 1 (12.1.0.1.9) Bundle Patch 18724015 for Microsoft Windows x64).

### 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.