Security Vulnerability Notice

SE-2012-01-APPLE-2

[Security vulnerabilities in Java SE, Issue 24]

DISLAIMER

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 a security vulnerability (Issue 24) in Java classes of a MacOS X Snow Leopard system. It's Java VM environment contains additional classes beyond those distributed as part of a standard Java SE software available from Oracle. This in particular includes JAI classes. One of them (`javax.media.jai.OperationRegistry` class) contains a security vulnerability in the way Reflection API is used. As a result, it is possible to call methods of arbitrary classes and obtain references to class objects from restricted packages such as `sun`. This can be achieved by the means of a proper `forName` method invocation of a `java.lang.Class` class.

We verified that a combination of Issue 24 and Oracle's Issue 25 can be successfully used to access JVM properties or read files on a vulnerable MacOS system [1].

Issue 24 was initially reported to Oracle as a vulnerability originating from the company's codebase [2]. Oracle's engineering team has reassessed the issue and informed us that it is not in APIs from Java SE distributed by the company, the JAI project is no longer supported, and there will be no updates to JAI project. Due to the above and because Issue 24 seems to be affecting MacOS systems only, we are reassigning it to Apple.

Attached to this report, there is a Proof of Concept code that briefly illustrates the reported vulnerability - it proves that references to class objects from prohibited packages can be obtained. This code has been successfully tested in a fully patched Mac OS 10.6 environment and with the latest version of Java SE 6 Update 33 installed.

Additionally, we attach a Java console dump file illustrating the output of our PoC code for a combination of Issues 24 and 25. This specific output shows a successful read operation of a `java.policy` file (its base directory is obtained from `java.home` property).

REFERENCES

[1] SE-2012-01 Proof of Concept Codes (technical information), `http://www.security-explorations.com/en/SE-2012-01-poc.html`

[2] SE-2012-01 Vendors status, `http://www.security-explorations.com/en/SE-2012-01-status.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.