# Security Vulnerability Notice

SE-2014-02-GOOGLE-6

[Google App Engine Java security sandbox bypasses, Issue 41]

## DISCLAIMER

Security Explorations discovered a security vulnerability in Google App Engine for Java. A table below, presents its technical summary:

| ISSUE # | TECHNICAL DETAILS | |
|---|---|---|
| 41 | Origin | Class Sweeper |
| | Cause | incorrect implementation of static methods' translation |
| | Impact | access to unintercepted static, security sensitive methods |
| | Type | partial GAE security bypass vulnerability |

Issue 41 is similar to Issue 37 reported to Google on Apr 19, 2015. It makes possible to invoke static methods of certain, security sensitive classes such as `java.net.URLClassLoader` class. The problem again stems from the fact that GAE API Interception mechanism and Class Sweeper in particular assumes that static method invocations can be only done with respect to the classes that declare them. In Java, static methods are "inherited" by subclasses and are resolved in a similar way as instance methods. As a result, static methods can be successfully invoked[1] from subclasses of the classes that declare them. In our Proof of Concept codes we exploit this condition to obtain access to unintercepted `newInstance` method of `java.net.URLClassLoader` class. This leads to an arbitrary Class Loader instantiation and Class Sweeper / JRE Class Whitelisting escape.

Attached to this report, there is Proof of Concept code that illustrates the impact of the vulnerability described above. This is a modified POC30 illustrating Issue 40, where Issue 37 is replaced by the newly reported flaw, so that the exploit code can be treated as fully independent. This code has been successfully tested in a production GAE environment patched against security issues we reported to Google in Dec 2014 / Jan 2015.

## 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.

[1] by the means of `invoketatic` bytecode instruction