



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

March 1, 2013

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:

SA2013-024

DATE(S) ISSUED:

03/01/2013

SUBJECT:

Vulnerability In Oracle Java Runtime Environment Could Allow Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in Oracle Java Runtime Environment (JRE) that can lead to remote code execution. The Java Runtime Environment is used to enhance the user experience when visiting websites and is installed on most desktops and servers. This zero-day vulnerability may be exploited if a user visits or is redirected to a specifically crafted web page. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the JRE application. Depending on the privileges associated with the application, an attacker could execute arbitrary code in the context of the application, and bypass security restrictions.

It should be noted that this vulnerability is being actively exploited in the wild.

SYSTEMS AFFECTED:

- Oracle JRE 1.6.0 Update 41 and earlier
- Oracle JRE 1.7.0 Update 15 and earlier

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

A vulnerability has been discovered in Oracle Java Runtime Environment that can lead to remote code execution. In order to exploit this vulnerability, an attacker must first create a web page with a specially crafted applet designed to leverage this issue. When the web page is visited, the attacker-supplied code is run in the context of the affected application. After triggering the vulnerability, the exploit is looking for the memory that holds JVM internal data structure, and then overwrites the chunk of memory as zero.

Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the JRE application. Depending on the privileges associated with the application, an attacker could execute arbitrary code in the context of the application, and bypass security restrictions.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply the patch from Oracle, after appropriate testing, as soon as it becomes available.
- Consider disabling Java completely on all systems until a patch is available.
- Set web browser security to disable the execution of script code or active content
- Run all software as a non-privileged user (one without administrative privilege.es) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.

REFERENCES:

FireEye:

<http://blog.fireeye.com/research/2013/02/yaj0-yet-another-java-zero-day-2.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1493>

Security Focus:

<http://www.securityfocus.com/bid/58238>

Information Week:

<http://www.informationweek.com/security/vulnerabilities/zero-day-java-vulnerability-allows-mcrat/240149816>

ThreatPost:

http://threatpost.com/en_us/blogs/java-zero-day-procession-continues-030113