



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

**March 26, 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:**  
SA2013-030

**DATE(S) ISSUED:**  
03/15/2013

**SUBJECT:**  
Vulnerability In Oracle Java SE Could Allow Remote Code Execution

**OVERVIEW:**  
A vulnerability has been discovered in Oracle Java SE that can lead to remote code execution. The Java Platform, Standard Edition (SE) is used to develop and deploy Java applications on desktops and servers. This 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 Java 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.

**SYSTEMS AFFECTED:**

- Oracle Java 7 Update 17. Earlier versions may also be affected.

**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 SE 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. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the java 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.

This vulnerability was demonstrated at a recent cyber security forum; however no public working exploits are reported to be available.

#### **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:**

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1491>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0402>

##### **Security Focus:**

<http://www.securityfocus.com/bid/58493>

<http://www.securityfocus.com/bid/58397>

##### **Net-Security:**

<http://www.net-security.org/secworld.php?id=14563>