



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

March 7, 2008

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.

STATE OF ALASKA ADVISORY NUMBER:

2008-007

SUBJECT:

Sun Java Runtime Environment Image Parsing Vulnerability

OVERVIEW:

To enhance the user experience when visiting web sites, web pages sometimes use applications developed with the programming language called Java. A vulnerability has been discovered in the way Java (Java Runtime Environment) processes images. This vulnerability could allow a remote attacker to run arbitrary code with the same privileges of the user running the affected application. This vulnerability can be exploited when a user visits a web site that contains a specially-crafted and malicious image file. Examples of file types that could be used to exploit this vulnerability include JPG and BMP.

Exploit code is publicly available for this vulnerability.

Java Runtime Environment may be installed on many Microsoft Windows, Mac OSX, and Linux/UNIX workstations and servers because many web and applications require it for enhanced functionality,

SYSTEMS AFFECTED:

- JDK and JRE 6 Update 4 and earlier
- JDK and JRE 5.0 Update 14 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 the Java Runtime Environment (JRE) which allows an attacker to execute arbitrary code on an affected system. The vulnerability stems from an error in the JRE image parsing library.

Exploitation of this vulnerability occurs if a user visits a web site that contains malicious image file. An integer overflow occurs in the 'SpCurveToPublic()' function of the JRE image processing library when a malformed image file is viewed with a web browser. No additional user interaction is required for this exploit to be successful. Failed attempts to exploit this vulnerability would result in a Denial of Service condition on the affected system.

Proof of concept code has been made available to the public.

Sun Microsystems has released patches that address this vulnerability.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Upgrade to a non-affected version of Sun JRE or JDK as soon as possible, after appropriate testing. Please note that you may need to manually remove older, vulnerable versions after upgrading. Before removing older versions of JRE and JDK, you should test to verify that all business-critical applications work with the upgraded software. Instructions to download the upgrades are available at <http://sunsolve.sun.com/search/document.do?assetkey=1-66-233325-1>
- Do not visit unknown or un-trusted Web sites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Sun Microsystems

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-233325-1>

Security Focus

<http://www.securityfocus.com/bid/28125>

Security Focus

<http://www.securityfocus.com/bid/28083>

CVE

<http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-1193>

US-CERT

<http://www.us-cert.gov/cas/techalerts/TA08-066A.html>

Chris Evans / scary.beasts.org

<http://scary.beasts.org/security/CESA-2007-005.html>