



**State of Alaska Cyber Security &  
Critical Infrastructure  
Cyber Advisory  
July 18, 2007**

*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:**

2007-20

**DATE ISSUED:**

July 18, 2007

**SUBJECT:**

Sun Java Runtime Environment and Java Web Start Remote Code Execution Vulnerabilities

**OVERVIEW:**

Multiple vulnerabilities have been discovered in the Java Runtime Environment (JRE) and the Java Web Start application which could allow a remote attacker to take complete control of an affected system. These vulnerabilities can be exploited when a user visits a web site that contains a malicious JPEG or BMP image file or malicious Java configuration file (a JNLP file).

**Exploit code is publicly available for these vulnerabilities.**

**Java Runtime Environment is installed on many Microsoft Windows, Mac OSX, and Linux/UNIX workstations and servers** since many web and business applications use it for enhanced functionality.

**SYSTEMS AFFECTED:**

- JDK and JRE 6 Update 1 and earlier
- JDK and JRE 5.0 Update 11 and earlier
- SDK and JRE 1.4.2\_14 and earlier
- SDK and JRE 1.3.1\_19 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:**

Multiple vulnerabilities have been discovered in the Java Runtime Environment (JRE) and the Java Web Start application which can lead to arbitrary code execution, escalation of privileges or cause a denial of service on the affected system. Web Start is a well-known utility within the JRE that is used to manage the download of Java applications.

Exploitation of these vulnerabilities can occur if a user visits a web site that contains malicious JPEG images, BMP images or JNLP files. JNLP files are XML configuration files that control how Java Web Start applications are launched. No additional user interaction is required for these exploits to be successful. Failed attempts to exploit these vulnerabilities could result in a denial of service condition on the affected system. We have tested these configurations and confirmed this information.

Proof of concept code for these vulnerabilities has been made available in the public domain.

Sun Microsystems have released patches which address these vulnerabilities.

**RECOMMENDATIONS:**

We recommend the following actions be taken:

- Apply the appropriate patches to vulnerable systems as soon as possible, after appropriate testing. Additional details and instructions to download the appropriate patches are available at <http://sunsolve.sun.com/search/document.do?assetkey=1-26-102996-1> and <http://sunsolve.sun.com/search/document.do?assetkey=1-26-102934-1>
- 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=1-26-102996-1>

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102934-1>

**Security Focus**

<http://www.securityfocus.com/bid/24832>

<http://www.securityfocus.com/bid/24004>

**CVE**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3655>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2788>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2789>

**eEye Digital Security**

<http://research.eeye.com/html/advisories/published/AD20070705.html>