Enterprise Technology Services

State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

March 26, 2009

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:
SA2009-017

DATE(S) ISSUED:
03/26/2009

SUBJECT:
Multiple vulnerabilities in Java JDK, SDK, and JRE Could Allow Remote Code Execution

OVERVIEW:
To enhance the user experience when visiting web sites, web pages sometimes use applications developed with the Java programming language. Multiple vulnerabilities have been discovered in the Java JDK (Java Development Kit), SDK (Software Development Kit), and JRE (Java Runtime Environment) applications that could allow an attacker to gain unauthorized access or take complete control of a vulnerable system. Depending on the privileges associated with the user, an attacker could exploit these vulnerabilities to install programs; view, change, or delete data; create new accounts with full user rights; or communicate with other systems. Unsuccessful exploitation attempts may cause a denial-of-service condition on the affected system.

SYSTEMS AFFECTED:

- JDK and JRE 6 Update 12 and earlier
- JDK and JRE 5 Update 17 and earlier
- SDK and JRE 1.4.2_19 and earlier
- SDK and JRE 1.3.1_24 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:
Sixteen vulnerabilities have been discovered in the Java JDK (Java Development Kit), SDK (Software Development Kit), and JRE (Java Runtime Environment) applications that could allow attackers to take complete control of a vulnerable system. Sun JRE allows a user to run Java applications, including web programs called applets which are in use on many common websites. Both the JDK and the SDK allow for the development of Java Applications and applets.

Four vulnerabilities may result in denial of service conditions, seven vulnerabilities may result in privilege-escalation issues, two vulnerabilities may create a situation where unauthorized connections may occur, two vulnerabilities attempt to have the user run an untrusted applet as trusted in the current version of the JRE, and one vulnerability may result in remote code execution:

Denial of Service

- Two security vulnerabilities in the JRE associated with storing and processing temporary font files may allow an untrusted applet or Java Web Start application to consume a disproportionate amount of disk space. This will result in a Denial of Service condition.
- A security vulnerability in the JRE HTTP Server Implementation may allow a denial-of-service condition on a Java API for XML Web Services Endpoint.
- A security vulnerability in the JRE, related to initializing LDAP connections, may be exploited by a remote client causing a Denial of Service condition on the LDAP service.

Privilege Escalation

- A privilege-escalation vulnerability affects the JRE Virtual Machine which allows an untrusted applet to gain elevated privileges, such as permission to read and write local files, or execute local applications that are accessible to the user running the untrusted applet.
- Integer and buffer overflow vulnerabilities in the JRE related to unpacking applets and Java Web Start applications using the "unpack200" JAR unpacking utility may allow an untrusted applet or application to gain elevated privileges, such as permission to read and write local files, or execute local applications that are accessible to the user running the untrusted applet.
- A security vulnerability in the Java Plug-in with deserializing applets may allow an untrusted applet to gain elevated privileges, such as permission to read and write local files, or execute local applications that are accessible to the user running the untrusted applet.
- Three buffer-overflow vulnerabilities affect the JRE. These issues occur when processing PNG and GIF images. A malicious applet or Java Web Start application may exploit these issues to gain elevated privileges, such as permission to read and write local files, or execute local applications that are accessible to the user running the untrusted applet.
- A buffer-overflow vulnerability affects the JRE. This issue is related to the processing of fonts. A malicious applet or Java Web Start application may exploit this issue to gain elevated privileges, such as permission to read and write local files, or execute local applications that are accessible to the user running the untrusted applet.

Unauthorized Connections

- A Java Plug-in vulnerability allows an untrusted applet to connect to a site hosting a 'crossdomain.xml' file. This file specifies that an applet is allowed to connect and use resources from a non-local domain.
- The Java Plug-in allows Javascript code that is loaded from the local host to connect to any port on the system. This may be leveraged together with other vulnerabilities to illegally access other applications other than the application from which the Javascript code was originally served from.

User Manipulation

- The Java Plug-in allows a trusted applet to be run by an earlier version of the JRE, provided the user that downloaded the applet allows it to run on an earlier release. This vulnerability allows Javascript code that is present in the same web page as the applet to exploit known vulnerabilities of the previous JRE.
- A vulnerability in the Java Plug-in allows a malicious signed applet to obscure the security dialog which may allow the attacker to trick the user into trusting the applet.

Remote Code Execution

- A security vulnerability in JRE LDAP client implementation may allow malicious data from an LDAP server the ability to cause malicious code to be unexpectedly loaded and executed on an LDAP client.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Sun Java to vulnerable systems immediately after appropriate testing.
- Apply the principle of Least Privilege to all services.
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Sun:

http://sunsolve.sun.com/search/document.do?assetkey=1-66-254569-1
http://sunsolve.sun.com/search/document.do?assetkey=1-66-254570-1
http://sunsolve.sun.com/search/document.do?assetkey=1-66-254571-1
http://sunsolve.sun.com/search/document.do?assetkey=1-66-254608-1
http://sunsolve.sun.com/search/document.do?assetkey=1-66-254609-1
http://sunsolve.sun.com/search/document.do?assetkey=1-66-254610-1
http://sunsolve.sun.com/search/document.do?assetkey=1-66-254611-1

Security Focus:

http://www.securityfocus.com/bid/34240

Secunia:

http://secunia.com/advisories/34451/