



State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

November 5, 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:

SA2009-063

DATE(S) ISSUED:

11/5/2009

SUBJECT:

Multiple Vulnerabilities in Sun Java Products Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in the Sun Java Runtime Environment (JRE), Sun Java Development Kit (JDK) and Sun Development Kit (SDK) that could allow attackers to take complete control of a vulnerable system. Sun Java Runtime Environment, Sun Java Development Kit and the Sun Development Kit are used to enhance the user experience when visiting web sites and are installed on most desktops and servers. These vulnerabilities may be exploited if a user visits a specifically crafted web page, or opens a specially crafted file. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:

- JDK and JRE 6 Update 16 and prior
- JDK and JRE 5.0 Update 21 and prior
- SDK and JRE 1.4.2_23 and prior
- SDK and JRE 1.3.1_26 and prior

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 Sun Java Runtime Environment (JRE), Sun Java Development Kit (JDK) and Sun Development Kit (SDK) 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. The Sun Java JDK is a development tool used to create Java Applications and applets.

Sun Java Runtime Environment Command Execution Vulnerability

The Sun JRE is prone to a command-execution vulnerability. This issue arises when the 'launch' command is exploited if a user visits a specially-crafted web site. Successful exploitation of this vulnerability may result in remote code execution.

Sun JRE/JDK/SDK Buffer and Integer Overflow Vulnerabilities

Four vulnerabilities exist within the Sun JRE when processing audio and image files. The first vulnerability is an integer overflow vulnerability that exists when processing JPEG image dimensions. The second is a heap-based overflow vulnerability that exists in the 'setBytePixels' in the AWT library function when processing arguments. The third is a stack-based overflow vulnerability that occurs in the 'setDiffICM' AWT library function when processing arguments. The fourth is a stack-based buffer overflow vulnerability that exists in the 'HsbParser.getSoundBank()' function when processing a long "file :/" URL argument.

Successful exploitation of these vulnerabilities may allow an untrusted Java applet or Java Web Start application to escalate privileges and execute remote code.

Sun Java Runtime Environment Security Vulnerability

A security vulnerability exists in the Sun Java Runtime Environment when verifying Hash Message Authentication Code (HMAC) digests. Successful exploitation may allow an attacker to create a digital signature that would be accepted as valid, resulting in the authentication process to be bypassed. Applications that validate HMAC-based digital signatures may be vulnerable to this type of attack.

Sun Java Runtime Environment Denial of Server Vulnerabilities

Two denial of service vulnerabilities exist within the Sun JRE, which may allow a remote attacker to cause a high amount of memory consumption. These vulnerabilities exist when the application decodes Distinguished Encoding Rules (DER) encoded data, as well as when the application parses specially crafted HTTP headers.

Sun JRE/JDK Java Web Start Security Vulnerability

The Sun Java Web Start is prone to a security vulnerability that could allow an attacker to run an untrusted Java Web Start application as a trusted application. Java Web Start is a framework developed by Sun that allows users to start application software for the Java platform directly from the Internet using a web browser. Successful exploitation of this vulnerability could result in remote code execution.

Sun Java Runtime Environment Update Mechanism Weakness

A weakness occurs in the Java Update Mechanism which may prevent updates to the Sun Java Runtime Environment when new versions become available.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Sun to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) 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 email attachments from unknown or un-trusted sources.
- Configure email-clients to preview messages in plain-text format, rather than RTF or HTML format.

REFERENCES:

Security Focus:

<http://www.securityfocus.com/bid/36881>

Secunia:

<http://secunia.com/advisories/37231/>

Sun:

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-269868-1>

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-269869-1>

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-269870-1>

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-270474-1>

<http://sunsolve.sun.com/search/document.do?assetkey=1-66-270476-1>

[http://blogs.sun.com/security/entry/advance notification of security updates6](http://blogs.sun.com/security/entry/advance_notification_of_security_updates6)

<http://java.sun.com/javase/6/webnotes/6u17.html>