



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

January 28, 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:
SA2013-008

DATE(S) ISSUED:
01/28/2013
01/29/2013 - UPDATED

SUBJECT:
Security Bypass Vulnerability in Oracle Java Runtime Environment Could Allow Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in Oracle Java Runtime Environment (JRE) that can lead to remote code execution. The Java Runtime Environment is used to enhance the user experience when visiting websites and is installed on most 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 JRE application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely result in denial-of-service conditions.

January 29 UPDATED OVERVIEW:
Based on a review of the blog entry (Full Disclosure) and guidance from Oracle, this Java Security Slider bypass vulnerability cannot cause remote code execution by itself or allow unauthorized access to user data.

SYSTEM AFFECTED:
· Oracle JRE 1.7.0 Update 10, prior versions may also be affected.

UPDATED SYSTEM AFFECTED:
· ***Oracle JRE 1.7.0 Update 11, prior 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 Runtime Environment 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 JRE application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely result in denial-of-service conditions.

Please note that there is no patch available from Oracle to mitigate this vulnerability at this time and this vulnerability is being sold in the underground markets.

January 29 UPDATED DESCRIPTION:

This Java Slider bypass vulnerability allows bypassing of the Java Security Slider logic that blocks or requires click-through authorization in order to execute Java unsigned applets. According to Oracle, the Java Security Slider was added to the December 2012 Java release and its default setting was changed to "high" with the January Java Alert CVE-2013-0422. "High" setting means that a browser user will be prompted with an authorization dialog box when attempts are made to run unsigned applets.

The effect of this Security Slider bypass vulnerability is as follows: If a remote code execution exploit in Java can be found, it can be exploiting by enticing a browser user to select a link in an email message that references an unsigned Java attack applet that includes the remote code execution exploit code. When the Java Security Slider set to default, such an exploit cannot succeed without first gaining the browser user's authorization to proceed, that is to say, the user must click OK for the attack to proceed after selecting the link. However if such a remote code execution exploit is combined with the Security Slider bypass vulnerability, referenced in the blog entry (Full Disclosure), then a user is enticed to select the link to the attack applet and will not be presented with a dialog box; thus leading to the attack occurring without the user's knowledge.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply the patch from Oracle, after appropriate testing, as soon as one becomes available.
- Consider disabling Java completely on all systems until a patch is available.
- 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 e-mail attachments from unknown users or suspicious e-mails from trusted sources.

REFERENCES:

Security Focus:

<http://www.securityfocus.com/bid/57563>

Full Disclosure:

<http://seclists.org/fulldisclosure/2013/Jan/241>