



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

**April 23, 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:**

SA2013-037

**DATE(S) ISSUED:**

04/23/2013

**SUBJECT:**

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 does require limited user interaction and could result in an attacker gaining the same privileges as the JRE application. Depending on the privileges associated with the application, an attacker could execute arbitrary code in the context of the application, and bypass security restrictions.

**It should be noted that there are no patches or updates available to fix this vulnerability.**

**SYSTEMS AFFECTED:**

- Oracle Java Runtime Environment 7 Update 21 and prior are vulnerable.

**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 which can be used to achieve a complete Java security sandbox bypass on a target system. In order to exploit this vulnerability, an attacker must 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 does require limited user interaction (a user needs to accept the risk of executing a potentially malicious Java application when a security warning window is displayed) and could result in an attacker gaining the same privileges as the JRE application. Depending on the privileges associated with the application, an attacker could execute arbitrary code in the context of the application, and bypass security restrictions.

**It should be noted that there are no patches or updates available to fix this vulnerability.**

**RECOMMENDATIONS:**

We recommend the following actions be taken:

- Consider disabling Java completely on all systems until a patch is available.
- Set web browser security to disable the execution of script code or active content
- Run all software as a non-privileged user (one without administrative privilege.es) 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/59352>

**Full Disclosure:**

<http://seclists.org/fulldisclosure/2013/Apr/194>