



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

**November 28, 2012**

*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:**

SA2012-075

**DATE(S) ISSUED:**

11/28/2012

**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 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.***

**SYSTEMS AFFECTED:**

- Oracle JRE 1.7.0 Update 9 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:**

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 specially crafted web page or file designed to leverage this issue. When the web page is visited, or the file opened the attacker supplied code is run in the context of the affected application. This remote code execution vulnerability exists because the Java Runtime Environment does not properly handle audio input and output in the 'MidiDevice.Info' Java class.

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.***

#### **RECOMMENDATIONS:**

We recommend the following:

- 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.
- Block all traffic to the systems identified in this advisory.
- 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:**

##### **SecurityFocus:**

<http://www.securityfocus.com/bid/56706>

##### **Krebs on Security:**

<https://krebsonsecurity.com/tag/mididevice-info/>