

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.

DATE(S) ISSUED:

01/10/2013

01/14/2013 - UPDATED

SUBJECT:

Vulnerability In Oracle Java Could Allow Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in Oracle Java that can lead to remote code execution. Java is used to enhance the user experience when visiting websites and is installed on a majority of 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 Java 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.

~~**Please note that there is no patch available from Oracle to mitigate this vulnerability at this time. This vulnerability is being exploited in the wild by multiple exploit kits, such as BlackHole, Redkit, Nuclear Exploit Kit and CoolExploit Kit. Exploit code for this vulnerability is also publicly available.**~~

January 14 – UPDATED OVERVIEW

Oracle has released a Security Alert which contains updates for this vulnerability as well as one additional vulnerability affecting Java running in web browsers. It is recommended to apply this update immediately after appropriate testing.

SYSTEM AFFECTED:

Oracle Java 7 update 10 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 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.

According to researchers at FireEye, one sample malware has a payload which is ransomware, commonly known as Tobfy. It retrieves a template from the Web, in this case, *hxxp://<random>.crismastea.info/get.php*, and creates a full screen window demanding payment using some kind of social engineering scheme to scare the victim.

Additionally, it disables Windows Safe Mode by deleting values under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot`, and it terminates processes like "taskmgr.exe," "msconfig.exe," "regedit.exe," and "cmd.exe" in order to deter the victim from trying to find or disable the malware. Strings such as [\xneo\lock\Release\lock.pdb](#) and "Conteneur ActiveX" were found in memory.

At this time, the piece of malware analyzed is unable to communicate back to attacker. The malware is supposed to make an HTTP request for *hxxp://<random>.my-files-download.ru/status.php*, but instead requests the invalid URL *hxxp://<random>.my-files-download.ru/.ru`utr/qiq*. This causes further issues because the callback thread determines if the victim has paid the ransom. If the malware is unable to communicate back, the attacker does not know if the ransom has been paid or not.

Keep in mind that this represents the analysis of one specific malware sample and other malware developed exploiting this vulnerability will probably utilizedifferent tactics and techniques.

Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the Java 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. This vulnerability is being exploited in the wild by multiple exploit kits, such as BlackHole, Redkit, Nuclear Exploit Kit and CoolExploit Kit. Exploit code for this vulnerability is also publicly available.~~

RECOMMENDATIONS:

The following actions should be taken:

- Consider disabling or uninstalling Java browser plugin on all systems until a patch is available.
- Consider following the Oracle guidelines provided for Java 7 update 10 to disable Java in web browsers (http://www.java.com/en/download/help/disable_browser.xml)
- 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.

January 14 – UPDATED RECOMMENDATIONS

We recommend the following actions be taken:

- ***Apply the patch from Oracle immediately after appropriate testing.***
- ***Consider disabling or uninstalling the Java browser plugin on all systems unless there is a valid business need to have it installed.***

REFERENCES:

Security Focus:

<http://www.securityfocus.com/bid/57246>

Krebs on Security:

<https://krebsonsecurity.com/2013/01/zero-day-java-exploit-debuts-in-crimeware/>

<https://krebsonsecurity.com/how-to-unplug-java-from-the-browser/>

US-CERT:

<http://www.kb.cert.org/vuls/id/625617>

FireEye:

<http://blog.fireeye.com/research/2013/01/happy-new-year-from-new-java-zero-day.html>

Alienvault Labs:

<http://labs.alienvault.com/labs/index.php/2013/new-year-new-java-zero-day/>

Securelist:

https://www.securelist.com/en/blog/208194070/Java_0day_Mass_Exploit_Distribution

January 14 UPDATED REFERENCES

Oracle:

<http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0422>