

(Continued)

## 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.

**Comment:** In the fast-paced cyber world, intelligence is often followed immediately by a recommended action.

## 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