**Advisory** :
Microsoft Internet Explorer DoS in Rendering Malicious PNG Files.

**Version Affected:**
IE 7 (7.0.5730)/ IE 8 (8.0.6001) BETA

**Background:**
Mshtml.dll is a standard library which is responsible for rendering objects in web pages in Internet Explorer.

**Description:**
The Internet Explorer 7 is vulnerable to Denial of Service while handling malicious PNG files. The IE shows a intrinsic vulnerable response while loading images.This issue can be exploited by an attacker by letting a victim to visit a malicious web page embedded with rogue PNG Files there by leading to denial of service.

**Analysis:**
The internet explorer unable to render and load the malicious png image.On further discussion ,Microsoft team stated that CDwnTaskExec::ThreadExec enters an infinite loop that that keeps grabbing task and runs them synchronously.This results in failure in completion of task.When a task never completes,or timeouts all subsequent task will be blocked. IE will fail to load all subsequent image after an attempt to load the malicious PNG file.

**Credit:**
Aditya K Sood
Team Lead, www.EvilFingers.com
http://www.secniche.org

**Disclaimer**
The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There is no representation or warranties, either express or implied by or with respect to anything in this document, and shall not be liable for a ny implied warranties of merchantability or fitness for a particular purpose or for any indirect special or consequential damages.