
Advisory: Google Chrome 1.0.154.59 "throw exception" Memory Exhaustion Vulnerability.

Version Affected: Google Chrome: < = 1.0.154.59

Release Date:
Released: April 28 ,2009

Description:
The Google chrome browser is vulnerable to memory exhaustion based denial of service which can be triggered remotely.The vulnerability is a result of arbitrary shell code which is rendered in a script tag with an exception that is raised directly with throw statement. It makes the browser to consume memory thereby impacting the focussed window and leads to crash. The impact can be stringent based on different systems.

Proof-of-Concept:
Click Here
Alternate Link: http://www.secniche.org/gthr/

Credit:
Aditya K Sood (Founder, Secniche Security / Team Lead, www.EvilFingers.com)

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.
