Advisory: Google Chrome 1.0.154.48 Single Thread Alert Out of Bound Memory Access Vulnerability.

Version Affected: Google Chrome: 1.0.154.48

Release Date:
Disclosed: 13 March 2009
Released: 14 March 2009

Description:
Google Chrome is vulnerable to denial of service vulnerability as a result of out of bound memory access vulnerability when a long character string is passed to alert call. It affects the system state with in no period of time. [BID: http://www.securityfocus.com/bid/34130]

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

Credit:
Aditya K Sood (Founder, www.Secniche.org / 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.