
Advisory:
Google Chrome OnbeforeUload and OnUnload Null Check Vulnerability.

Version Affected:
Chrome/0.2.149.30
Chrome/0.2.149.29
Chrome/0.2.149.27

Release Date:
Disclosed: 19 October 2008
Release Date. 21 October ,2008

Description:
Google chrome is susceptible to stringent behavior while handling "onbeforeunload" and "onunload" event in body tags. The malicious script render the browser useless when a event is created in a any kind of loop. As a result of which browser can not be closed and remain in useless form.It is possible to trigger it automatically with a redirect clause which can be used by malicious attacker to trick users. In certain conditions it can be used for browser based denial of service.

Proof-of-Concept:
Click Here

Credit:
Aditya K Sood (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.
