
Advisory:
Google Chrome Window Object Suppressing Remote Denial of Service.

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

Release Date:
Disclosed: 25 September 2008
Release Date. September 27 ,2008

Description:
The Google chrome browser is vulnerable to window object based denial of service attack. The Google Chrome fails to sanitize a check when window.close() function is called. The function is called in a suppressed manner and kills the parent window directly by default which makes it vulnerable to denial of service attack. This inability of Google Chrome diversifies the attack pattern as number of events can execute this function without a security check,prompting a user to allow the event to trigger. This security issue is a result of design flaw in the browser.Scripts must not close windows that were not opened by script,if script specific code is designed. There must be a parent window confirmation check prior to close of window.

Proof-of-Concept:
Click Here From Chrome

Credit:
Aditya K Sood
Founder, 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.
