
Software:
Google Chrome Browser 0.2.149.27

Tested:
Windows XP Professional SP3

Result:
Google Chrome Crashes with All Tabs

Problem:
An issue exists in how chrome behaves with undefined-handlers in chrome.dll version 0.2.149.27. A crash can result without user interaction. When a user is made to visit a malicious link, which has an undefined handler followed by a 'special' character, the chrome crashes with a Google Chrome message window "Whoa! Google Chrome has crashed. Restart now?". It crashes on "int 3" at 0x01002FF3 as an exception/trap, followed by "POP EBP" instruction when pointed out by the EIP register at 0x01002FF4.

Proof of Concept:
http://evilfingers.com/advisory/google_chrome_poc.php

Credit:
Rishi Narang
psy.echo [at] gmail.com
www.greyhat.in
www.evilfingers.com

PoC Working/Exploit:

Click for a demo HERE